Handbuch zur Testversion
Überarbeitung 1.0

ePolicy Orchestrator® 3.5

Einfache Schritte zum Einrichten von ePolicy Orchestrator und kennen lernen von neuen Funktionen in einer Testumgebung

McAfee®
System Protection

Branchenweit führende Lösungen zum Schutz vor Eindringlingen

McAfee®

COPYRIGHT

Copyright © 2004 Networks Associates Technology, Inc. Alle Rechte vorbehalten.

Diese Publikation darf in keiner Form und in keiner Weise ohne die schriftliche Genehmigung von Networks Associates Technology, Inc., oder ihren Lieferanten und angeschlossenen Unternehmen ganz oder teilweise reproduziert, übertragen, transkribiert, in einem Abrufsystem gespeichert oder in eine andere Sprache übersetzt werden. Diese Genehmigung können Sie schriftlich bei der Rechtsabteilung von McAfee unter der folgenden Adresse beantragen: 5000 Headquarters Drive, Plano, Texas 75024, USA, oder telefonisch +1-972-963-8000.

MARKEN

Active Firewall, Active Security, ActiveSecurity (und in Katakana), ActiveShield, AntiVirus Anyware und Design, Clean-Up, Design (stilisiertes E), Design (stilisiertes N), Entercept, Enterprise SecureCast, Enterprise SecureCast (und in Katakana), ePolicy Orchestrator, First Aid, ForceField, GMT, GroupShield, GroupShield (und in Katakana), Guard Dog, HomeGuard, Hunter, IntruShield, Intrusion Prevention Through Innovation, M und Design, McAfee, McAfee (und in Katakana), McAfee und Design, McAfee.com, McAfee VirusScan, NA Network Associates, Net Tools, Net Tools (und in Katakana), NetCrypto, NetOctopus, NetScan, NetShield, Network Associates, Network Associates Colliseum, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, RingFence, Router PM, SecureCast, SecureSelect, SpamKiller, Stalker, ThreatScan, TIS, TMEG, Total Virus Defense, Trusted Mail, Uninstaller, Virex, Virus Forum, ViruScan, VirusScan, VirusScan (und in Katakana), WebScan, WebShield, WebShield (und in Katakana), WebStalker, WebWall, What's The State Of Your IDS?, Who's Watching Your Network, Your E-Business Defender, Your Network. Our Business. sind eingetragene Marken von McAfee, Inc., und/oder der Tochterunternehmen in den USA und anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit ist ein Merkmal der McAfee®-Produkte. Alle anderen registrierten und nicht registrierten Marken in diesem Dokument sind alleiniges Eigentum der jeweiligen Besitzer.

PATENTINFORMATION

Geschützt durch die US-Patente 6,470,384; 6,493,756; 6,496,875; 6,553,377; 6,553,378.

INFORMATIONEN ZUR LIZENZ

Lizenzvereinbarung

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DER BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT (ALS BROSCHÜRE, DATEI AUF DER PRODUKT-CD ODER ALS DATEI, DIE VON DER SEITE, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESER VEREINBARUNG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. SOFERN MÖGLICH, GEBEN SIE DAS PRODUKT AN MCAFEE ODER IHREN HÄNDLER BEI VOLLER RÜCKERSTATTUNG DES KAUFPREISES ZURÜCK.

Hinweise

Dieses Produkt enthält oder enthält möglicherweise:

♦ Software, die im Projekt "OpenSSL" zur Verwendung im OpenSSL Toolkit entwickelt wurde (http://www.openss1.org/). ♦ Kryptographie-Software von Eric Young und Software von Tim J. Hudson. ♦ Einige Softwareprogramme, für die der Benutzer eine Lizenz (oder Unterlizenz) unter GNU General Public License (GPL) oder anderen ähnlichen freien Softwarelizenzen hält, die es dem Benutzer u. a. erlauben, bestimmte Programme oder Teile davon zu kopieren, zu ändern und weiterzuverbreiten, und die Zugriff auf den Quellcode gewähren. Bei Software, die GPL unterliegt und in ausführbarem Binärformat an andere Personen weitergegeben wird, muss diesen Benutzern auch der Quellcode zur Verfügung gestellt werden. Der Quellcode der GPL unterliegenden Software ist auf dieser CD einsehbar. Wenn Lizenzen für freie Software erfordern, dass McAfee Rechte zum Nutzen, Kopieren oder Ändern eines Softwareprogramms einräumt, die über die in diesem Vertrag genannten Rechte hinausgehen, dann haben die Rechte bezüglich freier Software Vorrang gegenüber den im Vertrag genannten Rechten. ♦ Ursprünglich von Henry Spencer geschriebene Software. Copyright 1992, 1993, 1994, 1997 Henry Spencer. ♦ Ursprünglich von Robert Nordier geschriebene Software. Copyright © 1996-7 Robert Nordier. ♦ Von Douglas W. Sauder geschriebene Software. ♦ Von Apache Software Foundation geschriebene Software (http://www.apache.org/). Eine Kopie der Lizenzvereinbarung zu dieser Software finden Sie unter www.apache.org/licenses/LICENSE-2.0.txt. ♦ International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation und andere. ♦ Von CrystalClear Software, Inc., geschrieben Software. Copyright © 2000 CrystalClear Software, Inc. ♦ FEAD® Optimizer®-Technologie, Copyright Netopsystems AG, Berlin. ♦ Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. und/oder Outside In® HTML Export, © 2001 Stellent Chicago, Inc. ♦ Software, die zugunsten von Thai Open Source Software Center Ltd. und Clark Cooper urheberrechtlich geschützt ist, © 1998, 1999, 2000. ♦ Software, die zugunsten von Expat maintainers urheberrechtlich geschützt ist. ♦ Software, die zugunsten von The Regents of the University of California urheberrechtlich geschützt ist, © 1989. ♦ Software, die zugunsten von Gunnar Ritter urheberrechtlich geschützt ist. ♦ Software, die zugunsten von Sun Microsystems®, Inc urheberrechtlich geschützt ist, © 2003. ♦ Software, die zugunsten von Gisle Aas urheberrechtlich geschützt ist. © 1995-2003. ♦ Software, die zugunsten von Michael A. Chase urheberrechtlich geschützt ist, © 1999-2000. ♦ Software, die zugunsten von Neil Winton urheberrechtlich geschützt ist, © 1995-1996. ♦ Software, die zugunsten von RSA Data Security, Inc. urheberrechtlich geschützt ist, © 1990-1992. ♦ Software, die zugunsten von Sean M. Burke urheberrechtlich geschützt ist, © 1999, 2000. ♦ Software, die zugunsten von Martijn Koster urheberrechtlich geschützt ist, © 1995. ♦ Software, die zugunsten von Brad Appleton urheberrechtlich geschützt ist, © 1996-1999. ♦ Software, die zugunsten von Michael G. Schwern urheberrechtlich geschützt ist, © 2001. ♦ Software, die zugunsten von Graham Barr urheberrechtlich geschützt ist, © 1998. ♦ Software, die zugunsten von Larry Wall und Clark Cooper urheberrechtlich geschützt ist, © 1998-2000. ♦ Software, die zugunsten von Frodo Looijaard urheberrechtlich geschützt ist, © 1997. ♦ Software, die zugunsten der Python Software Foundation urheberrechtlich geschützt ist, © 2001, 2002, 2003. Eine Kopie der Lizenzvereinbarung zu dieser Software finden Sie unter www.python.org. ♦ Software, die zugunsten von Beman Dawes urheberrechtlich geschützt ist, © 1994-1999, 2002. ♦ Von Andrew Lumsdaine, Lie-Quan Lee und Jeremy G. Siek geschriebene Software, © 1997-2000 University of Notre Dame. ♦ Software, die zugunsten von Simone Bordet & Marco Cravero urheberrechtlich geschützt ist, © 2002. ♦ Software, die zugunsten von Stephen Purcell urheberrechtlich geschützt ist, © 2001. ♦ Von Indiana University Extreme! Lab (http://www.extreme.indiana.edu/) geschriebene Software. ♦ Software, die zugunsten der International Business Machines Corporation und anderen urheberrechtlich geschützt ist, © 1995-2003. ♦ Software von der University of California, Berkeley und Beitragenden. ♦ Software von Ralf S. Engelschall <rse@engelschall.com>, die zur Verwendung im Projekt "mod_ssl" entwickelt wurde (http://www.modssl.org/). ♦ Software, die zugunsten von Kevlin Henney urheberrechtlich geschützt ist, © 2000-2002. ♦ Software, die zugunsten von Peter Dimov und Multi Media Ltd. urheberrechtlich geschützt ist, © 2001, 2002. ♦ Software, die zugunsten von David Abrahams urheberrechtlich geschützt ist, © 2001, 2002. Dokumentation hierzu finden Sie unter http://www.boost.org/libs/bind/bind.html. ♦ Software, die zugunsten von Steve Cleary, Beman Dawes, Howard Hinnant und John Maddock urheberrechtlich geschützt ist, © 2000. ♦ Software, die zugunsten von by Boost.org urheberrechtlich geschützt ist, © 1999-2002. ♦ Software, die zugunsten von Nicolai M. Josuttis urheberrechtlich geschützt ist, © 1999. ♦ Software, die zugunsten von by Jeremy Siek urheberrechtlich geschützt ist, © 1999-2001. ♦ Software, die zugunsten von Daryle Walker urheberrechtlich geschützt ist, © 2001. ♦ Software, die zugunsten von Chuck Allison und Jeremy Siek urheberrechtlich geschützt ist, © 2001, 2002. ♦ Software, die zugunsten von Samuel Krempp urheberrechtlich geschützt ist, © 2001. Aktualisierungen, Dokumentation und den Versionsverlauf finden Sie unter http://www.boost.org. ♦ Software, die zugunsten von Doug Gregor (gregod@cs.rpi.edu) urheberrechtlich geschützt ist, © 2001, 2002. ♦ Software, die zugunsten von Cadenza New Zealand Ltd. urheberrechtlich geschützt ist, © 2000. ♦ Software, die zugunsten von by Jens Maurer urheberrechtlich geschützt ist, © 2000, 2001. ♦ Software, die zugunsten von Jaakko Järvi (jaakko.jarvi@cs.utu.fi) urheberrechtlich geschützt ist, © 1999, 2000. ♦ Software, die zugunsten von Ronald Garcia urheberrechtlich geschützt ist, © 2002. ♦ Software, die zugunsten von David Abrahams, Jeremy Siek und Daryle Walker urheberrechtlich geschützt ist, © 1999-2001. ♦ Software, die zugunsten von Stephen Cleary (shammah@voyager.net) urheberrechtlich geschützt ist, © 2000. ♦ Software, die zugunsten von Housemarque Oy <http://www.housemarque.com> urheberrechtlich geschützt ist, © 2001. ♦ Software, die zugunsten von Paul Moore urheberrechtlich geschützt ist, © 1999. ♦ Software, die zugunsten von Dr. John Maddock urheberrechtlich geschützt ist, © 1998-2002. ♦ Software, die zugunsten von Greg Colvin und Beman Dawes urheberrechtlich geschützt ist, © 1998, 1999. ♦ Software, die zugunsten von Peter Dimov urheberrechtlich geschützt ist, © 2001, 2002. ♦ Software, die zugunsten von Jeremy Siek und John R. Bandela urheberrechtlich geschützt ist, © 2001. ♦ Software, die zugunsten von Joerg Walter und Mathias Koch urheberrechtlich geschützt ist, © 2000-2002.

Inhalt

Einführung: Bevor Sie beginnen 5

Schritt 1: Installieren des ePolicy Orchestrator-Servers und der Konsole 10
Schritt 2: Erstellen eines Verzeichnisses von verwalteten Computern 13
1. Hinzufügen von Computern zum Verzeichnis 14
2. Organisieren von Computern für Server und Workstations in Gruppen 18
Schritt 3: Pushen der Agenten auf Clients in Ihrem Verzeichnis 20
1. Konfigurieren der Agentenrichtlinien vor dem Ausbringen 21
2. Starten einer Agenteninstallation auf den Computern an Ihrem Standort . 22

Manuelles Installieren des Agenten auf den Client-Computern 23
Schritt 4: Einrichten des Master-Repositorys und anderen verteilten Repositories 25
1. Hinzufügen von VirusScan Enterprise zum Master-Repository 26
2. Abrufen von Aktualisierungen aus dem McAfee Quell-Repository. 27
3. Erstellen eines verteilten Repositories 29
    1. Erstellen eines gemeinsam genutzten Ordners auf einem Computer als Repository 29
    2. Hinzufügen des verteilten Repositorys zum ePolicy Orchestrator-Server 30
    3. Replizieren von Daten vom Master-Repository auf die verteilten Repositories 32
    4. Konfigurieren der Remote-Site für das verteilte Repository 33
Schritt 5: Festlegen von VirusScan Enterprise 8.0i-Richtlinien vor der Ausbringung 34
Schritt 6: Ausbringen von VirusScan Enterprise auf Clients 36
Schritt 7: Ausführen einen Berichts, um den Schutzumfang zu bestätigen . . 39
Schritt 8: Aktualisieren von DAT-Dateien mit einer geplanten Client-Aktualisierung. 40
Schritt 9: Planen der automatischen Repository- Synchronisierung 42
1. Planen eines Pull-Tasks, um Ihr Master-Repository täglich zu aktualisieren 43
2. Planen eines Replikations-Tasks zum Aktualisieren Ihres verteilten Repositorys 44
3. Planen eines Client-Aktualisierungs-Tasks, um DATs täglich zu aktualisieren. 45
Schritt 10: Testen von globaler Aktualisierung mit SuperAgents 45
1. Ausbringen eines SuperAgent auf jedes Subnet 46
2. Aktivieren der globalen Aktualisierung auf dem ePolicy Orchestrator-Server 47
Schritt 11: Wie geht es jetzt weiter? 48

Testen der Funktionen 49

ePolicy Orchestrator-Benachrichtigung 49
Schritt 1: Konfigurieren von Agentenrichtlinien, um Ereignisse sofort hochzuladen 50
Schritt 2: Konfigurieren von Benachrichtigungen 51
Schritt 3: Erstellen einer Regel für ein beliebiges VirusScan Enterprise-Ereignis 52
Schritt 4: Ermöglichen einer beispielhaften Virusentdeckung 54

Entdeckung nicht autorisierter Systeme 55
Schritt 1: Konfigurieren von Richtlinien zu Sensoren für die Entdeckung nicht autorisierter Systeme. 56
Schritt 2: Ausbringen des Sensors für die Entdeckung nicht autorisierter Systeme 57
Schritt 3: Konfigurieren einer automatischen Antwort 59
Schritt 4: Entdecken und Behandeln nicht autorisierter Rechner 61

Einführung: Bevor Sie beginnen

Dieses Handbuch zur Testversion zeigt, wie Sie ePolicy Orchestrator in einer Testumgebung installieren und ausbringen können. Es enthält einfache Schritte zu einer schnellen Einrichtung einer Testausbringung von ePolicy Orchestrator 3.5 und veranschaulicht wichtige Funktionen.

Dieses Handbuch ist in zwei Abschnitte unterteilt:

- Installation und Setup
- Verwalten und Überwachen Ihrer Umgebung

Zehn einfache Schritte, um ePolicy Orchestrator zu installieren und VirusScan Enterprise auszubringen

In diesem Handbuch zur Testversion werden die folgenden Schritte behandelt:

1 *Installieren des ePolicy Orchestrator-Servers und der Konsole*.

2 *Erstellen eines Verzeichnisses von verwalteten Computern*.

3 *Pushen der Agenten auf Clients in Ihrem Verzeichnis*.

4 *Einrichten des Master-Repositorys und anderen verteilten Repositories*.

5 *Festlegen von VirusScan Enterprise 8.0i-Richtlinien vor der Ausbringung*.

6 *Ausbringen von VirusScan Enterprise auf Clients*.

7 *Ausführen einen Berichts, um den Schutzumfang zu bestätigen*.

8 *Aktualisieren von DAT-Dateien mit einer geplanten Client-Aktualisierung*.

9 *Planen der automatischen Repository- Synchronisierung*.

10 *Testen von globaler Aktualisierung mit SuperAgents*.

Inhalt dieses Handbuchs

In diesem *Handbuch zur Testversion* wird beschrieben, wie ePolicy Orchestrator 3.5 in einer kleinen Laborumgebung mit einem ePolicy Orchestrator-Server und einer geringen Anzahl von Client-Computern ausgebracht wird. Es werden die notwendigen Schritte zum schnellen Ausbringen von ePolicy Orchestrator in einer solchen Umgebung und zum Testen der wichtigsten Funktionen aufgezeigt.

Einschränkungen dieses Handbuchs

In diesem Handbuch werden nicht alle Möglichkeiten von ePolicy Orchestrator dargestellt, z. B. erweiterte Funktionen oder typische Installationsszenarien wie sie in realen Ausbringungen durchgeführt werden. Sie können sich für Ihre eigene Umsetzung der Ausbringung an diese grundlegenden Schritte halten. In diesem Handbuch werden jedoch möglicherweise nicht alle für Sie wichtigen Punkte behandelt. Verwenden Sie das *ePolicy Orchestrator 3.5 Produkthandbuch*, um einen vollständigen Überblick über alle produktspezifischen Aspekte einschließlich erweiterter Funktionen zu erhalten.

Inhalt dieses Handbuchs zur Testversion

Behandeltes Thema	Nicht behandeltes Thema	Anmerkungen
Einzelner ePolicy Orchestrator-Server und Konsole	Mehrere ePolicy Orchestrator-Server und Remote-Konsolen	In einer kleinen Testumgebung ist ein einzelner Server ausreichend.
MSDE-Datenbank auf demselben Server, auf dem ePolicy Orchestrator ausgeführt wird	SQL Server-Datenbanken oder Remote-Datenbankserver	Zum Testen in einem kleiner Labornetzwerk ist es einfacher, die zusammen mit ePolicy Orchestrator enthaltene MSDE-Datenbank zu verwenden.
Verwenden von ePolicy Orchestrator zum Ausbringen von Agenten und von VirusScan Enterprise	Verwenden von Anmeldeskripts oder Tools von Drittherstellern zum Ausbringen von Agenten und von VirusScan Enterprise an Client-Computern	Das manuelle Installieren des Agenten wird ebenfalls behandelt.
Einfache Netzwerkumgebung mit einer NT-Domäne und Active Directory	Unix-, Linux- oder Netware-Umgebungen	In diesem Handbuch werden die Hauptmerkmale des Produkts anhand von NT-Domänen und Active Directory dargestellt.

Einrichten der Laborumgebung zum Testen von ePolicy Orchestrator

Erstellen Sie vor dem Installieren und Testen von ePolicy Orchestrator ein sicheres Testnetzwerk. Das Planen und Testen einer realen Ausbringung in Ihrem Unternehmen nimmt möglicherweise Wochen oder sogar Monate in Anspruch, besonders bei sehr großen Unternehmen. Eine kleine Testumgebung können Sie jedoch innerhalb weniger Stunden einrichten. Das Bestimmen einiger in Ihrem Netzwerk vorhandener Computer zum Testen nimmt sogar noch weniger Zeit in Anspruch.

Als Mindestanforderung sollte in dieser Umgebung ein Server vorhanden sein, auf dem sich der ePolicy Orchestrator-Server befindet, sowie mindestens ein Client-Computer (Server oder Workstation), auf dem Sie Agenten und VirusScan Enterprise 8.0i ausbringen. Vollständige Informationen zu Software- und Hardwareanforderungen für den ePolicy Orchestrator-Server, den Agenten und VirusScan Enterprise 8.0i finden Sie im *ePolicy Orchestrator 3.5 Installationshandbuch* und im *VirusScan Enterprise 8.0i Installationshandbuch*.

Stellen Sie beim Einrichten der Testumgebung sicher, dass Ihr Netzwerk für ePolicy Orchestrator korrekt konfiguriert ist. Beachten Sie dabei die folgenden Punkte:

1 **Erstellen Sie ein Netzwerk-Benutzerkonto mit Administratorrechten**. Wenn Sie den ePolicy Orchestrator-Server zum "Pushen" von Agenten an Computer verwenden möchten, müssen auf dem Server Anmeldeinformationen für ein Administratorkonto vorhanden sein. Sie können die Verwendung dieser Anmeldeinformationen für ePolicy Orchestrator entweder bei der Serverinstallation einrichten oder beim "Pushen" des Agenten angeben. In jedem Fall benötigen Sie den Benutzernamen und das Kennwort eines Administrators, wenn Sie Agenten von der ePolicy Orchestrator-Konsole ausbringen möchten.

2 **Erstellen Sie vertauenswürdige Domänenverbindungen zu allen Remote-NT-Domänen**. Wenn Sie das Ausbringen von Agenten auf Computer außerhalb der lokalen NT-Domäne (der Domäne, in der sich der ePolicy Orchestrator-Server befindet) testen möchten, müssen Sie eine vertrauenswürdige Verbindung zwischen diesen Domänen erstellen. Diese Verbindung wird benötigt, damit der Server auf diese Remote-Clients Agenten ausbringen und Software installieren kann. Weitere Informationen zu diesem Thema finden Sie in der Dokumentation von Microsoft Windows. Außerdem benötigen Sie ein Benutzerkonto mit Administratorrechten in der Remote-Domäne, damit der ePolicy Orchestrator-Server Agenten auf Clients in dieser Domäne ausbringen kann.

3 **Führen Sie vom ePolicy Orchestrator-Server aus eine Ping-Abfrage der Client-Computer durch**. Testen Sie die Netzwerkverbindungen, indem Sie von dem Computer, auf dem der ePolicy Orchestrator-Server installiert werden soll, eine Ping-Abfrage der Client-Computer durchführen, auf die Agenten ausgebracht werden sollen. Öffnen Sie auf Ihrem Server ein Befehlsfenster. Wählen Sie dazu **Start** | **Ausführen** aus, und geben Sie dann in das Eingabefeld `cmd` ein. Geben Sie nun Ping-Befehle ein, und verwenden Sie dabei die unten angegebene Syntax. Testen Sie sowohl den Computernamen als auch die IP-Adresse:

```
ping MeinComputer

ping 192.168.14.52
```

4 **Stellen Sie sicher, dass die NT-Admin$-Freigabeordner der Clients vom Server aus zugänglich sind**. Testen Sie von dem Computer aus, auf dem Sie den ePolicy Orchestrator-Server installieren möchten, den Zugang zum standardmäßigen Freigabeordner `Admin$` auf jedem Client-Computer. Der ePolicy Orchestrator-Serverdienst benötigt Zugriff auf diesen freigegebenen Ordner, um Agenten und andere Software wie VirusScan Enterprise installieren zu können. Bei diesem Test werden auch Ihre Administratorberechtigungen bestätigt, denn ohne Administratorrechte können Sie nicht auf Remote-Freigaben vom Typ `Admin$` zugreifen. So gehen Sie vor, um vom ePolicy Orchestrator-Server aus auf `Admin$`-Freigaben zuzugreifen:

   a Wählen Sie **Start** | **Ausführen** aus.

   b Geben Sie in die Ausführungszeile den Pfad zur `Admin$`-Freigabe des Clients ein. Dazu geben Sie entweder den Computernamen oder die IP-Adresse ein, z. B.:

```
\\MeinComputer\Admin$

\\192.168.14.52\Admin$
```

Wenn die Computer ordnungsgemäß über das Netzwerk verbunden sind, umfassen Ihre Anmeldeinformationen genügend Rechte, und der freigegebene Ordner `Admin$` ist vorhanden. Es sollte ein Dialogfeld von Windows Explorer angezeigt werden.

5 **Installieren Sie Microsoft-Updates auf allen Client-Computern mit dem Betriebssystem Windows 95, Windows 98 oder Windows Me**. Wenn Ihre Tests auch Clients mit Windows 95, Windows 98 oder Windows Me umfassen, laden Sie die Aktualisierungen `VCREDIST.EXE` und `DCOM 1.3` von der Microsoft-Website herunter und installieren sie nach Bedarf auf jedem Client. Ohne diese Updates können ePolicy Orchestrator-Agenten auf den Clients nicht ausgeführt werden. Weitere Informationen hierzu entnehmen Sie dem *ePolicy Orchestrator 3.5 Produkthandbuch* oder den folgenden Links:

   support.microsoft.com/directory/article.asp?ID=KB;DE-DE;Q259403&

   www.microsoft.com/com/dcom/dcom95/dcom1_3.asp

6 **Aktivieren Sie die Datei- und Druckerfreigabe auf allen Client-Computern mit dem Betriebssystem Windows 95, Windows 98 oder Windows Me**. Wenn Sie den Agenten auf Clients mit Windows 95, Windows 98 oder Windows Me ausbringen möchten, müssen Sie auf diesen Clients zuerst die **Datei- und Druckerfreigabe** aktivieren. Dies ist nur erforderlich, wenn Sie Agenten auf diese Clients *pushen* möchten. Wenn Sie den Agenten manuell oder über eine andere Methode installieren (z. B. über ein Anmeldeskript), ist dies nicht erforderlich. Sie können die **Datei- und Druckerfreigabe** wieder deaktivieren, nachdem Sie den Agenten mittels Push-Verfahren an diese Clients mit Windows 95, Windows 98 oder Windows Me übertragen haben, und die Agentenrichtlinien dann mit ePolicy Orchestrator weiter auf diesen Clients verwalten.

Informationen zu der in diesem Handbuch verwendeten Laborumgebung

Die in diesem Handbuch verwendete Laborumgebung besteht aus einer NT-Domäne und einem Active Directory-Container, die jeweils mehrere Server und mehrere Workstations enthalten.

Für die Verwendung dieses Handbuchs oder das Testen von ePolicy Orchestrator ist es nicht notwendig, dass die Laborumgebung mehrere NT-Domänen oder Active Directory-Container enthält.

Tabelle 1 Computer in Domäne1 (IP-Adressen 192.168.14.1-255)

Computer	Details
ePO-Server	Windows 2000 Server SP 4 mit SQL Server 2000 SP 3. Auf diesem Computer befinden sich ePolicy Orchestrator Server, Konsole, Datenbank und das Master-Software-Repository.
4 Clients	Windows 2000 Professional als Betriebssystem.

Tabelle 2 Computer in Domäne2 (IP-Adressen 192.168.15.1-255)

Computer	Details
2 Server	Windows 2000 Server mit SP 4.
3 Clients	Windows 2000 Professional als Betriebssystem.

Erhalten der Installationsdateien von McAfee

Die benötigten Installationsdateien für ePolicy Orchestrator und VirusScan Enterprise erhalten Sie auf der McAfee-Website oder von der Produkt-CD, wenn Sie eine solche besitzen. Wenn Sie für Ihre Tests die 30-Tage-Testversionen verwenden möchten, laden Sie diese von der McAfee-Website herunter. Sie benötigen die folgenden Dateien:

- **EPO350EML.ZIP**. Die benötigten Installationsdateien für ePolicy Orchestrator 3.5-Server, -Konsole, und -Datenbank.
- **VSE800EEN.ZIP**. Die Installationsdateien für VirusScan Enterprise 8.0i, einschließlich der Package-Datei `PkgCatalog.z`, die für das Ausbringen von VirusScan Enterprise durch ePolicy Orchestrator verwendet wird.
- **VSC451Lens1.ZIP**. Die Installationsdateien für VirusScan 4.5.1 und die Datei `PkgCatalog.z`. VirusScan 4.5.1 benötigen Sie nur, wenn Sie Client-Computer mit Windows 95, Windows 98 oder Windows Me besitzen, da VirusScan Enterprise 8.0i unter diesen Betriebssystemen nicht funktioniert.

So laden Sie die Dateien von der McAfee-Website herunter:

1. Starten Sie auf dem Computer, auf dem Sie den ePolicy Orchestrator-Server und die Konsole installieren möchten, einen Browser, und öffnen Sie folgende Website:

   `http://www.mcafeesecurity.com/us/downloads/evals/`

2. Wählen Sie in der Liste den Eintrag **ePolicy Orchestrator Enterprise Edition 3.5** aus, und klicken Sie auf den Link **TRY**.
3. Füllen Sie das Formular aus, und befolgen Sie die Anweisungen, um die Datei EPO350EML.ZIP herunterzuladen.
4. Extrahieren Sie den Inhalt von EPO350EML.ZIP in einen temporären Ordner, z. B. C:\ePOTemp.
5. Wiederholen Sie diese Schritte, um die Testversion für VirusScan Enterprise 8.0i (VSE80iEVAL.ZIP) und VirusScan 4.5.1 (VSC451Lens1.ZIP) herunterzuladen.
6. Extrahieren Sie den Inhalt der heruntergeladenen ZIP-Dateien in einen temporären Ordner auf dem Computer, den Sie als ePolicy Orchestrator-Testserver verwenden möchten.

Während des in diesem Handbuch beschriebenen Ausbringungsprozesses müssen Sie mehrfach auf Dateien in diesen Ordnern zugreifen.

SCHRITT 1

Installieren des ePolicy Orchestrator-Servers und der Konsole

Installieren Sie den ePolicy Orchestrator-Server, die Konsole und Datenbank auf dem Computer, den Sie als ePolicy Orchestrator-Server verwenden möchten. In den Beispielen in diesem Handbuch wird der ePolicy Orchestrator-Server auf dem Computer *ePOServer* mit dem Betriebssystem Windows 2000 Server installiert.

So installieren Sie die ePolicy Orchestrator-Konsole und den Server:

1. Suchen und starten Sie die Datei SETUP.EXE, die sich im Stammverzeichnis des ePOTemp-Ordners befindet, aus dem Sie die Datei EPO350EML.ZIP extrahiert haben.
2. Klicken Sie auf der ersten Seite des Assistenten **Setup von ePolicy Orchestrator 3.5.0** auf **Weiter**.
3. Wenn Sie eine Testversion installieren, klicken Sie auf der Seite **Test** auf **OK**.
4. Wählen Sie im Lizenzvertrag **Ich akzeptiere die Bedingungen des Lizenzvertrags** aus, und klicken Sie auf **OK**.
5. Wählen Sie unter **Server und Konsole installieren** die **Installationsoptionen** aus, und klicken Sie auf **Weiter**. Falls erforderlich, können Sie auch den Installationsordner ändern.
6. Wenn ein Meldungsfeld anzeigt, dass Ihr Server nicht über eine statische IP-Adresse verfügt, ignorieren Sie dies, indem Sie auf **OK** klicken.

   Obwohl McAfee empfiehlt, ePolicy Orchestrator in Produktionsumgebungen auf einem Computer mit einer statischen IP-Adresse zu installieren, ist eine von DHCP-zugewiesene IP-Adresse für Testzwecke ausreichend.
7. Geben Sie in das Dialogfeld **Serverkennwort einstellen** das Kennwort ein, das Sie für den ePolicy Orchestrator-Server verwenden möchten. Sie können dieses Feld nicht leer lassen.
8. Deaktivieren Sie im Dialogfeld **Server-Dienstkonto** die Option **Lokales Systemkonto verwenden**.
9. Geben Sie im Bereich **Kontoinformationen** Domäne, Benutzername und ein Kennwort ein, die vom ePolicy Orchestrator-Server verwendet werden sollen.
10. Klicken Sie auf **Weiter**, um die Kontoinformationen zu speichern und fortzufahren.

Wenn das angegebene Konto kein Administratorkonto ist, wird ein Warnhinweis angezeigt, dass Sie ePolicy Orchestrator nicht zum Ausbringen von Agenten verwenden dürfen. Wenn der ePolicy Orchestrator-Server Rechte zum Ausbringen von Agenten haben soll, klicken Sie auf **OK** und anschließend auf **Zurück**, und geben ein Benutzerkonto und Kennwort mit Administratorrechten ein. Alternativ dazu können Sie ein Konto ohne Administratorrechte für den ePolicy Orchestrator-Server verwenden und dennoch Agenten ausbringen, indem Sie Berechtigungen eines Administrators zum Ausbringungszeitpunkt angeben. Schließlich können Sie auswählen, dass keine Agenten durch den ePolicy Orchestrator ausgebracht werden sollen, und stattdessen den Agenten manuell installieren und den ePolicy Orchestrator nur zur Richtlinienverwaltung verwenden. In diesem Fall benötigen Sie keine Administratorrechte für Ihr Server-Dienstkonto.

11 Wählen Sie im Dialogfeld **Datenbankserver auswählen** die Option **Einen Server auf diesem Computer installieren und verwenden** aus. Mit dieser Option wird die kostenfreie MSDE-Datenbank installiert, die in ePolicy Orchestrator enthalten ist.

12 Klicken Sie auf **Weiter**.

13 Deaktivieren Sie im Dialogfeld **Datenbankserver-Konto** die Option **Dasselbe Konto wie Serverdienst verwenden**, und wählen Sie anschließend die Option **Dies ist ein SQL-Serverkonto** aus. Geben Sie ein sicheres Kennwort ein, und überprüfen Sie es. Dies ist das SA-Konto, mit dem der ePolicy Orchestrator-Server auf die MSDE-Datenbank zugreift.

14 Klicken Sie auf **Weiter**, um die Kontoinformationen der Datenbank zu speichern.

15 Ändern Sie im Dialogfeld **HTTP-Konfiguration** den **Agenten-HTTP-Port** in **82** und den **Konsolen-HTTP-Port** in **83**.

Abbildung 1-1 Ändern des von Agent und Konsole verwendeten HTTP-Ports, wenn sie bereits verwendet werden

Setup von ePolicy Orchestrator 3.5.0
ePolicy Orchestrator 3.5
HTTP-Konfiguration
Der ePolicy Orchestrator-Server kommuniziert mit der Konsole und dem Agenten über HTTP. Damit diese Komponenten zusammenarbeiten können, müssen die HTTP-Ports auf den Workstations frei sein, die mit dem Server verwaltet werden sollen, sowie auf dem System, das den Server hostet.
Wenn Sie Workstations in einer anderen Domäne verwalten möchten, muss ein korrektes Weiterleiten von HTTP-Paketen über den Router sichergestellt sein.
Geben Sie die Port-Nummern, die Sie verwenden möchten, in die Textfelder ein.
Agenten-HTTP-Port: 82
Konsolen-HTTP-Port: 83
Agenten-Reaktivierung-HTTP-Port: 8081
Agenten-Broadcast-HTTP-Port 8082
Discovery & HTTP-Port für Benachrichtigungsdienst: 8080
Discovery & HTTPS-Port für Benachrichtigungsdienst: 8443
HTTPS-Port für Sensor für nicht autorisierte Systeme: 8444
McAfee SECURITY
< Zurück
Weiter >
Abbrechen

Einige HTTP-Ports, besonders die Ports 80 und 81, werden häufig von vielen HTTP-Anwendungen und -Diensten verwendet. Aus diesem Grund wird Port 80 möglicherweise bereits verwendet und steht nicht zur Verfügung. Sie sollten die Port-Nummer ändern, um diesen Konflikt zu vermeiden.

16 Klicken Sie auf **Weiter**, um die Port-Informationen zu speichern.

Wenn eine Warnmeldung angezeigt wird, dass mindestens ein HTTP-Port verwendet wird, klicken Sie auf **OK**, und wiederholen Sie Schritt 15, wobei Sie dieses Mal nicht benutzte HTTP-Ports angeben.

17 Geben Sie im Dialogfeld **E-Mail-Adresse festlegen** die E-Mail-Adresse ein, an die die standardmäßigen Benachrichtigungsregeln Nachrichten senden sollen, nachdem sie aktiviert sind.

Diese E-Mail-Adresse wird von der ePolicy Orchestrator-Benachrichtigungsfunktion verwendet. Diese Funktion wird in dem hier beschriebenen Beispiel beschrieben. Geben Sie daher eine E-Mail-Adresse ein, die Nachrichten empfängt.

18 Klicken Sie im Dialogfeld **Installationsbereit** auf **Installieren**, um die Installation zu starten.

Die Installation dauert etwa 20 Minuten und fordert Sie möglicherweise dazu auf, den Computer während des Installationsprozesses neu zu starten.

19 Klicken Sie auf **OK**, wenn Sie zum Neustart aufgefordert werden. Melden Sie sich nach dem Neustart unbedingt wieder an, damit die Installation fortgesetzt werden kann.

20 Klicken Sie nach Abschluss der Installation auf **Fertig stellen**.

Nach Abschluss der Installation können Sie die ePolicy Orchestrator-Konsole öffnen, um mit dem Ausbringen von Agenten und Antivirenprodukten auf die Client-Computer in Ihrem Netzwerk zu beginnen.

Erstmaliges Starten der ePolicy Orchestrator-Konsole

Jetzt ist Ihr Server installiert und betriebsbereit. Öffnen Sie die ePolicy Orchestrator-Konsole, um mit ePolicy Orchestrator Richtlinien auf Ihrem Netzwerk zu verwalten.

So öffnen Sie die Konsole über den ePolicy Orchestrator-Server:

1 Klicken Sie auf die Schaltfläche **Start**, und wählen Sie anschließend **Programme** | **Network Associates** | **ePolicy Orchestrator 3.5.0-Konsole** aus.

2 Klicken Sie auf der **Startseite** auf **Bei Server anmelden**.

3 Vergewissern Sie sich im Dialogfeld **Bei Server anmelden**, dass der **Servername** den Namen Ihres ePolicy Orchestrator-Servers anzeigt und als **Benutzername** `administrator` angegeben ist. Geben Sie anschließend das **Kennwort** ein, das Sie mit dem Installationsassistenten festgelegt haben, und klicken Sie auf **OK**.

4 Wenn Sie eine Testversion installiert haben, klicken Sie auf dem Begrüßungsbildschirm auf der Seite **Test** auf **OK**.

Warten Sie, bis der ePolicy Orchestrator-Server initialisiert ist. Nun können Sie die ePolicy Orchestrator-Konsole verwenden.

Sie haben ePolicy Orchestrator-Server, -Konsole und -Datenbank erfolgreich installiert. Herzlichen Glückwunsch!

SCHRITT

2

Erstellen eines Verzeichnisses von verwalteten Computern

Das **Verzeichnis** befindet sich auf der linken Seite der Struktur der ePolicy Orchestrator-Konsole. Es enthält alle Computer in Ihrem Netzwerk, die Sie mit ePolicy Orchestrator verwalten. Das bedeutet, dass das **Verzeichnis** alle Computer in Ihrem Netzwerk enthält, die aktive ePolicy Orchestrator-Agenten ausführen, die an diesen Server berichten.

Bevor Sie Antivirenrichtlinien für Computer auf Ihrem Netzwerk verwalten, müssen Sie diese Computer Ihrem ePolicy Orchestrator-**Verzeichnis** hinzufügen. Nach der Installation des Servers muss sich zunächst ein Computer im **Verzeichnis** befinden – der ePolicy Orchestrator-Server selbst.

Zum Organisieren Ihrer Computer können Sie sie in logische Einheiten zusammenfassen, die auch *Standorte* und *Gruppen* genannt werden. Sie können eine Hierarchiestruktur von Standorten und Gruppen erstellen, ähnlich wie Sie eine Ordner-Hierarchie im Windows Explorer erstellen würden. Es ist sinnvoll nach Gruppen zu ordnen, da mithilfe von ePolicy Orchestrator die Richtlinien auf dieser Ebene definiert werden können. Sie können die Computer gemäß der Kriterien gruppieren, die für Ihr Unternehmen sinnvoll sind.

Dieses Handbuch verwendet drei allgemeine Gruppierungsebenen:

- **NT-Domäne**. Wenn Sie vorhandene NT-Netzwerkdomänen als Standorte verwenden, kann Ihr **Verzeichnis** schnell und einfach erstellt werden. Wenn Ihre **Verzeichnis-**Struktur Ihre Netzwerkstruktur widerspiegelt, müssen Sie sich außerdem nur eine statt zwei verschiedene Hierarchien merken.
- **Active Directory-Container**. Wenn Sie die Active Directory-Netzwerkcontainer als Standorte verwenden, lässt sich das **Verzeichnis** oder Teile davon schnell und einfach erstellen. Wenn Ihre **Verzeichnis-**Struktur Ihre Netzwerkstruktur widerspiegelt, müssen Sie sich außerdem nur eine statt zwei verschiedene Hierarchien merken.
- **Server und Workstations**. Möglicherweise möchten Sie separate Richtlinien für Produkte wie VirusScan Enterprise 8.0i konfigurieren, je nachdem, ob die Software auf einem Server oder einer Workstation ausgeführt wird. Sie müssen das **Verzeichnis** nicht in Gruppen aufteilen, insbesondere nicht für Tests in einer kleinen Laborumgebung. Sie können jedoch Gruppen verwenden, um mit dem Einstellen von Richtlinien für Computergruppen oder der Organisation Ihres **Verzeichnisses** zu experimentieren.

Andere typische Methoden der Gruppierung umfassen beispielsweise:

- **Geographische Abteilungen**. Wenn Sie über Standorte in verschiedenen Teilen der Welt oder verschiedenen Zeitzonen verfügen, kann es sinnvoll sein, Ihr ePolicy Orchestrator-**Verzeichnis** gemäß diesen Abteilungen aufzuteilen. Die Koordination einiger Richtlinien oder Tasks über mehrere Zeitzonen hinweg ist bedeutend einfacher, wenn Sie Ihre Computer an solchen Standorten platzieren.
- **Sicherheitsabteilungen**. Wenn Benutzer Zugriff auf mehrere Sicherheitsebenen in Ihrer Umgebung haben, können Richtlinien bedeutend einfacher umgesetzt werden, wenn die **Verzeichnis-**Struktur so erstellt wird, dass diese Ebenen widergespiegelt werden.

1 Hinzufügen von Computern zum Verzeichnis

Der erste Schritt beim Erstellen des **Verzeichnisses** besteht darin, Computer aus Ihrem Netzwerk hinzuzufügen. Wenden Sie dabei eine der folgenden drei Methoden an:

- *Option A: Automatisches Hinzufügen vollständiger NT-Domänen zum Verzeichnis.*. Sehr einfach und schnell. Diese Methode ist sehr nützlich, wenn Sie die Ausbringung von Agenten auf allen Computern in dieser Domäne planen. Setzen Sie sie ein, wenn Sie den Test-Client-Computer in Ihrem Labornetzwerk in Domänen organisieren möchten, wie anhand der Beispiele in diesem Handbuch dargestellt.
- *Option B: Automatisches Hinzufügen der vollständigen Active Directory-Container zum Verzeichnis*. Sehr einfach und schnell. Diese Methode ist sehr nützlich, wenn Teile oder Ihre gesamte Umgebung von Active Directory gesteuert werden und Teile des ePolicy Orchestrator-**Verzeichnisses** Teile Ihrer Active Directory-Struktur widerspiegeln sollen.
- *Option C: Manuelles Hinzufügen einzelner Computer zum Verzeichnis*. Diese Methode ist möglicherweise zu langsam, wenn ePolicy Orchestrator in einem Netzwerk ausgebracht werden soll. Sie ist jedoch schnell genug, wenn Sie Ihrem Testnetzwerk nur einige Computer hinzufügen möchten.

Option A: Automatisches Hinzufügen vollständiger NT-Domänen zum Verzeichnis.

Mithilfe von ePolicy Orchestrator können Sie Computer in einer NT-Domäne mit nur wenigen Mausklicks in das **Verzeichnis** importieren. Verwenden Sie diese Funktion, wenn der Test-Client-Computer in Ihrem Labornetzwerk in Domänen organisiert werden soll.

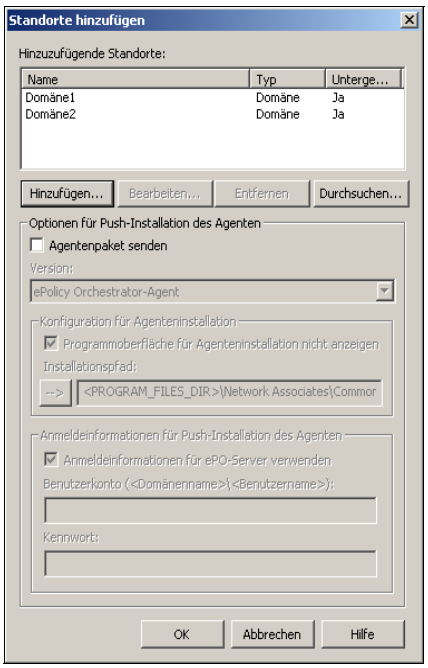
In den Beispielen in diesem Handbuch wird diese Methode verwendet, um Standort-**Verzeichnisse** aus einer NT-Domäne im Testnetzwerk **Domäne1** zu erstellen.

So fügen Sie vollständige NT-Domänen zum **Verzeichnis** hinzu:

1. Klicken Sie mit der rechten Maustaste auf **Verzeichnis**, und wählen Sie **Neu** | **Standort** aus.
2. Klicken Sie im Dialogfeld **Standorte hinzufügen** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Neuer Standort** einen Namen für den Standort ein. Stellen Sie sicher, dass der eingegebene Name genau mit dem Namen Ihrer NT-Domäne übereinstimmt.
4. Wählen Sie unter **Typ** die Optionen **Domäne** und **Computer als untergeordnete Knoten einbeziehen** aus.
5. Klicken Sie unter **IP- Verwaltung** auf **Hinzufügen**, um einen IP-Adressbereich für den Standort anzugeben.
6. Geben Sie im Dialogfeld **IP-Verwaltung** eine IP-Subnet-Maske oder einen IP-Bereich an, um die IP-Adressbereiche der Computer festzulegen, die zu diesem Standort gehören.
7. Klicken Sie auf **OK**, um die IP-Einstellungen zu speichern.
8. Klicken Sie auf **OK**, um den neuen Standort zu speichern und das Dialogfeld **Neuer Standort** zu schließen.

9 Stellen Sie sicher, dass im Dialogfeld **Standorte hinzufügen** die Option **Agentenpaket senden** NICHT ausgewählt ist, und klicken Sie auf **OK**, um Standorte im **Verzeichnis** zu erstellen und mit Daten zu füllen. Obwohl Sie zu diesem Zeitpunkt Agenten ausbringen können, werden Sie diese Aktion erst durchführen, wenn die Agenten-Richtlinien geändert wurden.

Abbildung 1-2 Dialogfeld "Standorte hinzufügen"



Nach einigen Augenblicken werden die Computer Ihrem **Verzeichnis** hinzugefügt. Wenn dies abgeschlossen ist, wird ersichtlich, dass ePolicy Orchestrator zuerst einen Standort im **Verzeichnis** mit dem Namen Ihrer Netzwerk-Test-Domäne erstellt und anschließend alle Computer in dieser Domäne als untergeordnete Elemente hinzugefügt hat.

Option B: Automatisches Hinzufügen der vollständigen Active Directory-Container zum Verzeichnis

Mithilfe von ePolicy Orchestrator können Sie alle Computer in einen Active Directory-Container und dessen Sub-Container mit nur wenigen Klicks in das **Verzeichnis** importieren. Verwenden Sie diese Funktion, wenn Ihre Test-Client-Computer in der Laborumgebung in Active Directory-Containern organisiert wurden.

In den Beispielen in diesem Handbuch wird diese Methode verwendet, um **Verzeichnis-**Standorte aus einem Active Directory-Container mit zwei Sub-Containern zu erstellen.

Wenn Sie die Active Directory-Tools von ePolicy Orchestrator verwenden, müssen sowohl der ePolicy Orchestrator-Server als auch der Computer mit der Remote-Konsole (sofern Sie eine solche verwenden) auf den Active Directory-Server zugreifen können.

Den **Assistenten für Active Directory-Import** wird zum erstmaligen Importieren von Active Directory-Computern verwendet, wobei Sie das gesamte **Verzeichnis** oder nur einen bestimmten Standort des **Verzeichnisses** erstellen. Mithilfe des Tasks **Active Directory Computer Discovery** fragen Sie diese Active Directory-Container später regelmäßig auf neue Computer ab.

So fügen Sie Active Directory-Container und Sub-Container zum **Verzeichnis** hinzu:

1 Klicken Sie mit der rechten Maustaste auf **Verzeichnis**, und wählen Sie **Neu** | **Standort** aus.

2 Klicken Sie im Dialogfeld **Standorte hinzufügen** auf **Hinzufügen**.

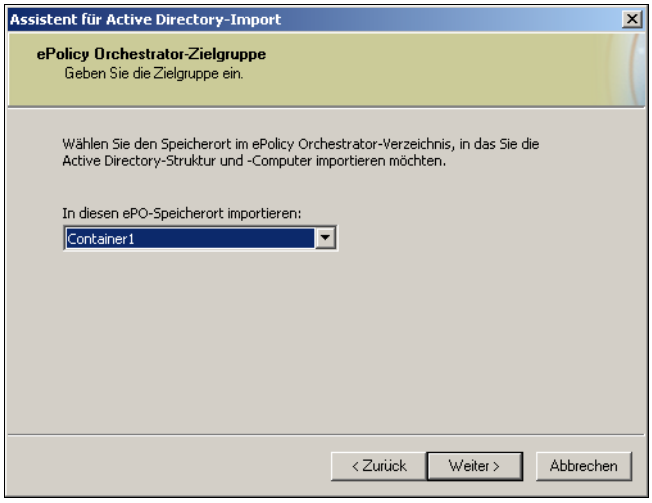
3 Geben Sie im Dialogfeld **Neuer Standort** einen Namen für den Standort ein, beispielsweise **Container1**, und klicken Sie anschließend auf **OK**.

4 Stellen Sie sicher, dass **Agentenpaket senden** NICHT aktiviert ist, und klicken Sie anschließend auf **OK**.

5 Klicken Sie mit der rechten Maustaste auf **Verzeichnis**, und wählen Sie **Alle Tasks** | **Active Directory-Computer importieren** aus.

6 Klicken Sie im **Assistenten für Active Directory-Import** auf **Weiter**.

Abbildung 1-3 Assistent für Active Directory-Import


Assistent für Active Directory-Import
ePolicy Orchestrator-Zielgruppe
Geben Sie die Zielgruppe ein.
Wählen Sie den Speicherort im ePolicy Orchestrator-Verzeichnis, in das Sie die Active Directory-Struktur und -Computer importieren möchten.
In diesen ePO-Speicherort importieren:
Container1
< Zurück
Weiter >
Abbrechen

7 Im Bereich **ePolicy Orchestrator-Zielgruppe** des Assistenten können Sie den **Verzeichnis**-Stamm oder den Standort des **Verzeichnisses** auswählen, um die Active Directory-Computer zu importieren.

Dem Beispiel in diesem Handbuch folgend wählen Sie den gerade erstellten Standort in der Dropdown-Liste **In diesen ePO-Speicherort importieren** aus und klicken anschließend auf **Weiter**.

Wenn Sie die gesamte Active Directory-Struktur (bis auf Ausnahmen) importieren und als ePolicy Orchestrator-**Verzeichnis** verwenden möchten, wählen Sie in der Liste **Stamm** aus. Dadurch wird die Active Directory-Struktur (bis auf die Ausnahmen) in den Ordner **Lost&Found** des **Verzeichnis**-Stamms importiert.

8 Geben Sie auf im Bereich **Active Directory-Authentifizierung** die Anmeldeinformationen für Active Directory mit Administratorrechten für den Active Directory-Server ein.

9 Klicken Sie im Dialogfeld **Active Directory-Quellcontainer** auf **Durchsuchen**, um den gewünschten Quellcontainer im Dialogfeld **Active Directory-Browser** auszuwählen, und klicken Sie anschließend auf **OK**.

10 Wenn Sie einen bestimmten Sub-Container des ausgewählten Containers ausschließen möchten, klicken Sie unter **Folgende Sub-Container ausschließen** auf **Hinzufügen**, wählen den auszuschließenden Sub-Container aus und klicken auf **OK**.

11 Klicken Sie auf **Weiter**, und zeigen Sie das Aktivitätsprotokoll für alle neu importierten Computer an. Überprüfen Sie in der ePolicy Orchestrator-Struktur, ob diese Computer importiert wurden.

12 Klicken Sie auf **Fertig stellen**.

Die Active Directory-Computer wurden in das Verzeichnis **Lost&Found** importiert, das sich unter dem Standort befindet, in den Sie sie importiert haben. Wenn Ihr Active Directory-Container Sub-Container enthielt, behält das Verzeichnis **Lost&Found** die Active Directory-Hierarchie bei.

13 Klicken Sie auf den oberen Bereich dieser Struktur, und verschieben Sie sie von **Lost&Found** in den übergeordneten Standort (in den Standort, den Sie im Assistenten ausgewählt haben, z. B. **Container1**).

Sie haben Ihre Active Directory-Computer in einen Standort im ePolicy Orchestrator-**Verzeichnis** importiert. Herzlichen Glückwunsch!

Wenn die Active Directory-Container importiert wurden, sollten Sie in einer Produktionsumgebung einen **Active Directory Computer Discovery**-Task erstellen. Dieser Task fragt regelmäßig administratorspezifische Active Directory-Container nach neuen Computern ab. Anleitungen hierzu finden Sie im *ePolicy Orchestrator 3.5 Produkthandbuch*. Dieser Task wird in diesem Handbuch nicht beschrieben.

Option C: Manuelles Hinzufügen einzelner Computer zum Verzeichnis

Wenn Sie ePolicy Orchestrator in Ihrem Produktionsnetzwerk ausbringen, möchten Sie unter Umständen das **Verzeichnis** automatisch mit Daten füllen, indem Sie Ihre NT-Domänen, wie im vorherigen Abschnitt dargestellt, importieren. Zu Testzwecken in einer kleinen Laborumgebung können Sie Standorte und Computer jedoch auch manuell zum **Verzeichnis** hinzufügen. Der erste Schritt besteht demnach darin, einen Standort zu erstellen. Anschließend können Sie manuell Computer hinzufügen.

Erstellen eines neuen Standortes, an dem die Computer in Gruppen eingeteilt werden sollen

1 Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den **Verzeichnisknoten**, und wählen Sie **Neu** | **Standort** aus.

2 Klicken Sie im Dialogfeld **Standorte hinzufügen** auf **Hinzufügen**.

3 Geben Sie im Dialogfeld **Neuer Standort** in das Feld **Name** einen Namen für den Standort ein, z. B. *Domäne1*.

4 Geben Sie, falls erforderlich, eine IP-Maske oder einen IP-Adressbereich für den Standort an. Weitere Informationen hierzu finden Sie im vorherigen Abschnitt.

5 Klicken Sie auf **OK**. Der Standort *Domäne1* wird zur Liste **Hinzuzufügende Standorte** im Dialogfeld **Standorte hinzufügen** hinzugefügt.

6 Wiederholen Sie, bei Bedarf, die vorherigen Schritte, um weitere Standorte zu erstellen.

7 Klicken Sie auf **OK**. ePolicy Orchestrator fügt die neuen, leeren Standorte zum **Verzeichnis** hinzu.

Manuelles Hinzufügen neuer Computer zum Standort

Nachdem Sie jetzt mindestens einen Standort erstellt haben, fügen Sie Ihrem Standort im nächsten Schritt jeden neuen Computer manuell hinzu. Führen Sie dazu folgende Schritte aus:

1 Klicken Sie im **Verzeichnis** mit der rechten Maustaste auf den hinzugefügten Standort und wählen **Neu** | **Computer** aus.

2 Fügen Sie im Dialogfeld **Computer hinzufügen** neue Computer hinzu, indem Sie entweder auf **Durchsuchen** klicken, um diese in Ihrer NT-Netzwerkumgebung zu finden, oder auf **Hinzufügen** und den Computernamen (NetBIOS-Namen) eingeben.

3 Klicken Sie auf **OK**, wenn Sie die Namen aller Computer hinzugefügt haben.

ePolicy Orchestrator fügt dem **Verzeichnis** die neuen Computer unterhalb des Standortes hinzu.

2 Organisieren von Computern für Server und Workstations in Gruppen

Wenn die Standorte erstellt sind und die Computer dem **Verzeichnis** hinzugefügt wurden, ist es sinnvoll, sie in Gruppen zu organisieren. Die Gruppen werden so erstellt, wie es in Ihrem Netzwerk am günstigsten ist. Möglicherweise möchten Sie die Computer nach Funktionsbereichen (z. B. Verkauf, Marketing oder Entwicklung), geographischen Einheiten (z. B. Niederlassungen) oder Betriebssystem gruppieren.

Im Beispiel in diesem Handbuch werden an jedem Standort Gruppen für Server und Workstations erstellt. Sie können diese Gruppen später bei der Erstellung unterschiedlicher VirusScan Enterprise-Richtlinien für Server und Workstations verwenden.

Mit den VirusScan Enterprise 8.0i-Richtlinienseiten für ePolicy Orchestrator 3.5.0 können Sie separate Richtlinien für Server und Workstations festlegen, ohne dabei Gruppen zu erstellen. Das Gruppieren von Computern nach Betriebssystem demonstriert auf einfache Art und Weise, wie das Verwenden von **Verzeichnis**-Gruppen die Richtlinienverwaltung vereinfachen kann. Erstellen Sie bei Bedarf andere Arten von Gruppen, die Ihrem Testnetzwerk oder Ihren Anforderungen in Bezug auf die Richtlinienverwaltung mehr entsprechen.

So fügen Sie Standorten im **Verzeichnis** Gruppen und Computer hinzu:

1 Klicken Sie im **Verzeichnis** mit der rechten Maustaste auf den hinzugefügten Standort, und wählen Sie **Neu** | **Gruppe** aus.

2 Klicken Sie im Dialogfeld **Gruppen hinzufügen** auf **Hinzufügen**.

3 Geben Sie im Dialogfeld **Neue Gruppe** den Namen der `Workstation` in das Textfeld **Name** ein.

4 Wenn Sie in Ihrem Netzwerk Servern und Workstations bestimmte IP-Adressen zuweisen können, erstellen Sie einen IP-Bereich für die Gruppe. Beispielsweise haben die Server in Domäne1 der in diesem Handbuch dargestellten Testnetzwerke IP-Adressen zwischen 192.168.14.200 und 255 und Workstations in Domäne1 Adressen zwischen 192.168.14.1 und 199.

Beachten Sie, dass Sie auch eine IP-Maske auf dem übergeordneten Standort festlegen müssen. Die von Ihnen für die Gruppe festgelegte IP-Maske oder der IP-Bereich muss mit dem auf Standortebene angegebenen IP-Bereich übereinstimmen. In den in diesem Handbuch dargestellten Beispielen stimmen die Workstations und Server in Domäne1 mit dem Subnet 192.168.14.0/24 überein.

Beachten Sie auch, dass die IP-Verwaltung für Active Directory-Computer nicht erforderlich ist.

So legen Sie einen IP-Bereich für eine Gruppe fest:

a Klicken Sie im Dialogfeld **Neue Gruppe** unter **IP-Verwaltung** auf **Hinzufügen**.

b Geben Sie im Dialogfeld **IP-Verwaltung** eine IP-Subnet-Maske oder einen IP-Bereich an, um die IP-Adressbereiche der Computer festzulegen, die zu diesem Standort gehören.

c Klicken Sie auf **OK**, um die IP-Einstellungen zu speichern und das Dialogfeld **IP-Verwaltung** zu schließen.

5 Klicken Sie auf **OK**, um das Dialogfeld **Neue Gruppe** zu schließen. Die Gruppe wird der Liste **Hinzuzufügende Gruppen** hinzugefügt.

6 Klicken Sie im Dialogfeld **Gruppen hinzufügen** auf **OK**, um die Gruppen zum **Verzeichnis** hinzuzufügen.

Hinzufügen von Computern zu neu erstellten Gruppen

Sobald die neuen Gruppen im **Verzeichnis** angezeigt werden, können Sie die Computer von diesem Standort in die entsprechende Gruppe verschieben, so wie Sie auch Dateien im Windows Explorer verschieben können. Die Computer müssen einzeln in das **Verzeichnis** verschoben werden. Es können nicht mehrere Computer gleichzeitig ausgewählt werden. Alternativ können Sie jedoch mit der **Verzeichnis**-Suchfunktion mehrere Systeme verschieben. (Klicken Sie dazu mit der rechten Maustaste auf das **Verzeichnis**, und wählen Sie **Suche** aus.)

Wenn Sie Computer in Gruppen verschieben, können Sie die Meldung **IP-Integritätswarnung** ignorieren, indem Sie auf **OK** klicken.

Erstellen von zusätzliche Gruppen und Untergruppen nach Bedarf

Wiederholen Sie sämtliche Schritte, um eine Servergruppe für Ihren Standort, sowie weitere Gruppen von Servern und Workstations für andere Standorte zu erstellen, wenn diese vorhanden sind. Sie können auch Gruppen innerhalb von Gruppen erstellen. Beispielsweise verfügt das in diesem Handbuch dargestellte Testnetzwerk über Computer mit Windows 2000 und Windows 98. Aufgrund von Beschränkungen mit älteren Windows-Versionen müssen unterschiedliche Richtlinien für Computer mit Windows 98 festgelegt werden. Das Erstellen von *Win98* und *Win2K*-Untergruppen innerhalb unserer Workstation-Gruppe vereinfacht das Festlegen dieser unterschiedlichen Richtlinien.

Jetzt ist Ihr Test-**Verzeichnis** fertig gestellt. Sie haben Standorte und Computer entweder manuell oder durch das Importieren vorhandener NT-Domänen auf Ihr Netzwerk erstellt und hinzugefügt. Zudem haben Sie die Computer an jedem Standort in unterschiedliche Gruppen für Server und unterschiedliche Arten von Betriebssystemen auf Workstations aufgeteilt. Sie sind nun bereit für den nächsten Schritt – das Ausbringen von Agenten.

SCHRITT 3

Pushen der Agenten auf Clients in Ihrem Verzeichnis

Bevor Sie fortfahren können, die Client-Computer in Ihrem **Verzeichnis** zu verwalten, müssen Sie einen ePolicy Orchestrator-Agenten auf diesen Client-Computern installieren. Der Agent ist eine kleine Anwendung, die auf dem Client-Computer installiert ist und in bestimmten Abständen den ePolicy Orchestrator-Server auf Aktualisierungen und neue Anweisungen überprüft.

Zum Ausbringen des Agenten vom ePolicy Orchestrator-Server ist Folgendes erforderlich:

- **Ein Netzwerkkonto mit Administratorrechten**. Wenn Sie bei der Installation Ihres ePolicy Orchestrator-Serverdienstes Administratorberechtigungen angegeben haben, können Sie Agenten automatisch ausbringen. Anderenfalls müssen Sie beim Ausbringen entsprechende Berechtigungen angeben.
- **Domänenvertrauungsstellungen zu anderen NT-Domänen (bei Bedarf)**. Wenn Agenten außerhalb der lokalen NT-Domäne, auf der sich Ihr ePolicy Orchestrator-Server befindet, ausgebracht werden sollen, muss eine Vertrauensbeziehung zwischen der lokalen und der Zieldomäne konfiguriert sein.
- **Zusätzliche Microsoft-Updates auf Windows 95- und Windows 98-Computern**. Bei den ersten Versionen von Windows 95 und Windows 98 müssen Sie zusätzliche Microsoft Updates installieren, damit der ePolicy Orchestrator-Agent ausgeführt werden kann. Informationen zum Suchen und Installieren dieser Updates finden Sie im *ePolicy Orchestrator Installationshandbuch*. Die Updates müssen auf all diesen Systemen installiert werden, damit der Agent ausgeführt werden kann, auch wenn ePolicy Orchestrator nicht zum Ausbringen verwendet wird.
- **Aktivierte Datei- und Druckerfreigabe für Windows 95- und Windows 98-Computer**. Aktivieren Sie die **Datei- und Druckerfreigabe** auf jedem Client, auf den der Agent gepusht werden soll. Beachten Sie, dass es sich hier nur nur eine Anforderung handelt, den Agenten vom ePolicy Orchestrator-Server zu *pushen*, nicht um Richtlinien zu verwalten. Nach dem Ausbringen des Agenten auf einen Windows 95- oder Windows 98-Computer können Sie die Datei- und Druckerfreigabe deaktivieren.

Aus dem **Verzeichnis** in der ePolicy Orchestrator-Konsole können Sie den Agenten auf allen Computern an einem Standort gleichzeitig installieren. Senden Sie dazu einen Befehl "Agenten installieren" auf Standortebene. Aufgrund des Konzepts der *Vererbung* können Sie eine Agenteninstallation auf der Ebene des übergeordneten Standortes (oder der Gruppe) angeben, und alle untergeordneten Elemente (sowohl Gruppen als auch Computer) erben den Befehl.

In unserem Beispiel-**Verzeichnis** mit zwei Standorten werden separate Agenteninstallationen für jeden Standort initiiert. Diese beiden Agenten-installationsbefehle führen die Installation des Agenten auf allen Computern an diesen Standorten durch.

So bringen Sie Agenten auf einen Standort aus:

1 *Konfigurieren der Agentenrichtlinien vor dem Ausbringen*.

2 *Starten einer Agenteninstallation auf den Computern an Ihrem Standort*.

Alternativ können Sie den Agenten manuell vom Client-Computer installieren, wenn Sie ePolicy Orchestrator nicht zum Pushen des Agenten verwenden möchten. Weitere Informationen hierzu finden Sie unter *Manuelles Installieren des Agenten auf den Client-Computern* auf Seite 23.

1 Konfigurieren der Agentenrichtlinien vor dem Ausbringen

Sie können die Agenten mit den standardmäßigen Richtlinieneinstellungen ausbringen. Zu Testzwecken ändern Sie jedoch die Richtlinie, damit das Agenten-Taskleistensymbol im Windows-Systemfeld auf dem Client-Computer angezeigt werden kann. Somit legen Sie nicht nur Agentenrichtlinien fest, sondern können auch einfacher erkennen, wann sich der Agent auf Ihren Clients installiert hat. Wenn Sie diese Richtlinie auf der Standortebene ändern, gilt sie für alle Testcomputer, die als untergeordnete Elemente an diesem Standort existieren. Auf diese Weise können Sie die Richtlinienkonfiguration einmal ändern und anschließend auf allen Computern an diesem Standort ausbringen.

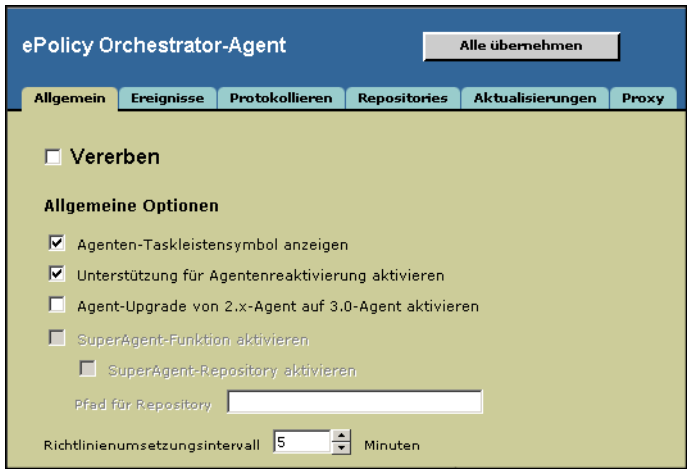
So ändern Sie die Agentenrichtlinie, damit das Agentensymbol nach der Installation in der Taskleiste angezeigt wird:

1 Wählen Sie Ihren Standort aus (in diesem Beispiel *Domäne1*), indem Sie in der **Verzeichnis**-Struktur einmal darauf klicken.

2 Klicken Sie im rechten Detailbereich auf die Registerkarte **Richtlinien**, und wählen Sie **ePolicy Orchestrator-Agent** | **Konfiguration** aus.

3 Deaktivieren Sie auf der Seite **ePolicy Orchestrator Agent** die Option **Vererben**, um die Konfigurationsoptionen zu aktivieren.

Abbildung 1-4 Registerkarte "Allgemein"



4 Aktivieren Sie auf der Registerkarte **Allgemein** die Option **Agenten-Taskleistensymbol**, und klicken Sie auf **Alle übernehmen**, um Ihre Änderung zu speichern.

5 Wiederholen Sie diese Schritte, um dieselben Änderungen für Agentenrichtlinien an anderen Standorten durchzuführen (in diesem Beispiel **Container1**).

Nun sind Ihre Richtlinien festgelegt und Ihre Agenten bereit für die Ausbringung. Im nächsten Schritt wird eine Agenteninstallation gestartet.

2 Starten einer Agenteninstallation auf den Computern an Ihrem Standort

Verwenden Sie die Funktion **Agenteninstallation**, damit ePolicy Orchestrator-Agenten auf die Client-Computer pusht. Sie können Agenten gleichzeitig auf alle Testcomputer an einem Standort pushen, indem Sie die Agenteninstallation auf der Standortebene im **Verzeichnis** initiieren.

So starten Sie eine Agenteninstallation für alle Computer an einem Standort:

1 Klicken Sie mit der rechten Maustaste in Ihr **Verzeichnis** und wählen **Agenteninstallation** aus.

2 Klicken Sie im Dialogfeld **Agenteninstallation** auf **OK**, um alle Standardeinstellungen zu akzeptieren und die Agenteninstallation zu starten.

Wenn Sie den ePolicy Orchestrator-Server installiert haben, um das lokale Systemkonto zu verwenden, müssen Sie die Option **Anmeldeinformationen für ePO-Server verwenden** deaktivieren und ein Benutzerkonto und Kennwort mit Administratorberechtigungen für Domänen angeben.

3 Wiederholen Sie diese Schritte für andere Standorte in Ihrem **Verzeichnis**.

Die Agenteninstallationen werden umgehend gestartet.

Ausbringen von Agenten auf Computern mit Windows 95, Windows 98 oder Windows Me

Beim Pushen der Agenten auf Computer mit Windows 95, Windows 98 oder Windows Me ist es unter Umständen nicht möglich festzustellen, ob der Agent erfolgreich ausgebracht wurde, bis Sie sich vom Client-Computer abgemeldet haben. Dazu gehört möglicherweise, dass das Agentensymbol nicht in der Taskleiste oder der Computer nicht im **Verzeichnis** der ePolicy Orchestrator-Konsole angezeigt werden. Wenn der Agent nach dem Abmelden und erneuten Anmelden bei Windows 95-, Windows 98- oder Windows Me-Clients immer noch nicht angezeigt wird, versuchen Sie ihn erneut zu pushen. Sollte dies dennoch nicht funktionieren, können Sie den Agenten manuell vom Client installieren (siehe hierzu auch *Manuelles Installieren des Agenten auf den Client-Computern* auf Seite 23).

Ausbringen auf Computern außerhalb der lokalen NT-Domäne

Wenn die anderen Standorte Computer enthalten, die sich in einer anderen NT-Domäne als Ihrem ePolicy Orchestrator-Server befinden, müssen Sie möglicherweise für die Zieldomäne andere Domänenadministratorberechtigungen angeben.

Bevor Sie das Pushen von Agenten initiieren, müssen Sie im Dialogfeld **Agenteninstallation** die Option **Anmeldeinformationen für ePO-Server verwenden** deaktivieren und einen entsprechenden Benutzernamen und ein Kennwort mit Domänenadministratorrechten in die Zieldomäne eingeben.

Was kann man während der Agenteninstallation tun?

Es dauert möglicherweise bis zu zehn Minuten, bis alle Agenten auf allen Computern an Ihren Standorten installiert sind und die **Verzeichnis**-Struktur mit dem neuen gedeckten Status aktualisiert ist. In der Zwischenzeit können Sie den ePolicy Orchestrator-Server auf Ereignisse überprüfen, der sie vor fehlgeschlagenen Agenteninstallationen warnen kann. So zeigen Sie Server-Ereignisse an:

1. Klicken Sie in der Struktur der ePolicy Orchestrator-Konsole mit der rechten Maustaste auf den Server, und wählen Sie **Server-Ereignisse** aus.
2. Blättern Sie die **Server-Ereignisanzeige** nach Ereignissen durch. Erfolgreiche Agenteninstallationen werden hier im Gegensatz zu fehlgeschlagenen Installationen nicht angezeigt.

Wenn die Ausbringung von Agenten abgeschlossen ist und sich die Agenten zum ersten Mal beim Server zurück gemeldet haben, werden die Computer in Ihrem **Verzeichnis** grün markiert.

Wenn die Agenten installiert wurden und das **Verzeichnis** dies nicht widerspiegelt, aktualisieren Sie es manuell, indem Sie mit der rechten Maustaste darauf klicken und **Aktualisieren** auswählen. Beachten Sie, dass das **Verzeichnis** die Computer nicht als verwaltet anzeigt, bis sie sich (meist innerhalb von zehn Minuten) beim Server zurückmelden. Dies trifft selbst dann zu, wenn der Agent installiert ist und auf den Clients ausgeführt wird.

Sie können die Installation von jedem Ihrer Client-Computer aus verfolgen. Die standardmäßige Richtlinie unterdrückt die Installations-Benutzeroberfläche (die in diesem Beispiel beim Erstellen von Agentenrichtlinien nicht geändert wurde). Daher können Sie die Benutzeroberfläche nicht sehen. Sie können jedoch den Task-Manager auf dem Client-Computer öffnen und beobachten, wie die CPU zu Beginn der Installation kurzzeitig voll ausgelastet ist. Nachdem der Agent installiert ist und ausgeführt wird, werden zwei neue Dienste im Fenster **Prozesse** angezeigt: `UPDATERUI.EXE` und `FRAMEWORKSERVICE.EXE`. Zudem wird aufgrund der Art und Weise, wie die Agentenrichtlinien vor der Ausbringung geändert wurden, das Agentensymbol nach der ersten Installation und Rückmeldung an den Servern der Taskleiste angezeigt.

Manuelles Installieren des Agenten auf den Client-Computern

Anstatt ePolicy Orchestrator zum Pushen des Agenten zu verwenden, möchten Sie diesen möglicherweise lieber manuell vom Client installieren. In einigen Unternehmen empfiehlt es sich unter Umständen, die Software manuell auf Clients zu installieren und ePolicy Orchestrator nur zur Verwaltung von Richtlinien heranzuziehen. Möglicherweise haben Sie aber auch viele Windows 95- oder Windows 98-Clients und möchten die Datei- und Druckfreigabe auf ihnen nicht aktivieren. In diesen Fällen können Sie den Agenten alternativ vom Client aus installieren.

Installieren Sie den Agenten mithilfe der Datei `FRAMEPKG.EXE`, die sich auf dem ePolicy Orchestrator-Server befindet. Die Datei `FRAMEPKG.EXE` wird automatisch erstellt, wenn Sie den ePolicy Orchestrator-Server installieren. Sie enthält Adressinformationen für Ihren ePolicy Orchestrator-Server, damit der neue Agent sofort mit dem Server kommunizieren kann.

Standardmäßig befindet sich FRAMEPKG.EXE im folgenden Ordner auf dem ePolicy Orchestrator-Server:

```
C:\Programme\Network Associates\ePO\3.5.0\DB\Software\Current\
  EPOAGENT3000\Install\0409
```

So führen Sie eine manuelle Installation des Agenten durch:

1. Kopieren Sie die Datei FRAMEPKG.EXE auf den lokalen Client- oder Netzwerkordner, der vom Client aus zugänglich ist.
2. Doppelklicken Sie die Datei FRAMEPKG.EXE, um Sie auszuführen. Warten Sie, während der Agent installiert wird.

Der Agent meldet sich in einem zufällig generierten Intervall innerhalb von zehn Minuten zum ersten Mal beim ePolicy Orchestrator-Server zurück. An dieser Stelle wird der Computer dem **Verzeichnis** als verwalteter Computer hinzugefügt. Falls Sie für die Standorte und Gruppen im **Verzeichnis** die Filterung nach IP-Adresse angegeben haben, wird der Client entsprechend seiner IP-Adresse dem entsprechenden Standort bzw. der Gruppe hinzugefügt. Andernfalls wird der Computer dem Ordner **Lost&Found** hinzugefügt. Sobald der Computer dem **Verzeichnis** hinzugefügt wurde, können Sie seine Richtlinien über die ePolicy Orchestrator-Konsole verwalten.

Sie können das zehnminütige Intervall umgehen und erzwingen, dass sich der neue Agent sofort beim Server zurückmeldet. Sie können dies von jedem Computer aus durchführen, auf dem soeben ein Agent installiert wurde.

So erzwingen Sie manuell die erste Rückmeldung des Agenten:

1. Öffnen Sie auf dem Client-Computer, auf dem Sie gerade den Agenten installiert haben, ein DOS-Befehlsfenster. Wählen Sie dazu **Start** | **Ausführen** aus, geben command ein und drücken die **Eingabetaste**.
2. Wechseln Sie im Befehlsfenster zum Installationsordner des Agenten, der die Datei CMDAGENT.EXE enthält.
3. Geben Sie den folgenden Befehl ein (beachten Sie die Leerzeichen zwischen den Befehlszeilenoptionen):

   ```
   CMDAGENT /p /e /c
   ```

4. Drücken Sie die **Eingabetaste**. Der Agent meldet sich sofort beim ePolicy Orchestrator-Server zurück.
5. Aktualisieren Sie auf dem Server in der ePolicy Orchestrator-Konsole das **Verzeichnis**, indem Sie **F5** drücken. Der neue Client-Computer, auf dem Sie gerade den Agenten installiert haben, sollte jetzt im **Verzeichnis** angezeigt werden.

SCHRITT

4

Einrichten des Master-Repositorys und anderen verteilten Repositories

Die Agenten sind nun auf Ihren Clients installiert, doch wozu dienen sie? Der Zweck eines Agenten besteht darin, die Verwaltung von Client-Sicherheitssoftware-Richtlinien zentral über ePolicy Orchestrator zu ermöglichen. Solange Sie jedoch keine Antivirensoftware auf Ihren Client-Computern installiert haben, haben Ihre Agenten nichts zu tun. Der nächste Schritt besteht darin, den ePolicy Orchestrator zur Ausbringung der Antivirensoftware VirusScan Enterprise 8.0i auf Ihren Client-Computern zu verwenden.

Software, die mit dem ePolicy Orchestrator ausgebracht werden soll, wird in Software-Repositories gespeichert. Es gibt viele Möglichkeiten, Ihre Repositories einzurichten. Dieses Handbuch beschreibt ein typisches Beispiel, das Sie in Ihrer Testumgebung verwenden können.

Weitere Einzelheiten hierzu finden Sie in den folgenden Abschnitten. Es werden die folgenden Schritte behandelt:

1 *Hinzufügen von VirusScan Enterprise zum Master-Repository*.

2 *Abrufen von Aktualisierungen aus dem McAfee Quell-Repository*.

3 *Erstellen eines verteilten Repositories*.

Verwenden von Master- und verteilten Repositories in Ihrem Netzwerk

ePolicy Orchestrator verwendet Repositories, um die Software zu speichern, die es ausbringt. Dieses Handbuch veranschaulicht sowohl die Verwendung von Master- als auch von verteilten Repositories zur Ausbringung von Software und zur Aktualisierung. Repositories speichern die Software (z. B. die Agenten- oder VirusScan-Installationsdateien) und Aktualisierungen (z. B. DAT-Dateien), die an die Clients ausgebracht werden sollen. Das Master-Repository befindet sich auf dem ePolicy Orchestrator-Server und ist der primäre Speicherbereich für Ihre Software und Aktualisierungen. Verteilte Repositories sind Kopien des Master-Repositories, die sich in anderen Teilen Ihres Netzwerks befinden können, z. B. Netzwerk-NT-Domänen oder andere Active Directory-Container. Computer in diesen anderen Teilen des Netzwerks können schneller von lokalen Servern aus aktualisiert werden als über ein WAN, das mit dem ePolicy Orchestrator-Server verbunden ist.

Domänen und Active Directory Container können über mehrere Standorte verteilt und über ein WAN verbunden sein. In diesem Fall erstellen Sie auf einem Computer an einem Remote-Standort ein verteiltes Repository, das eine Kopie des Master-Repositorys darstellt. Computer an diesem Standort (in unserem Beispiel **Container1**) können über das verteilte Repository aktualisieren anstatt Aktualisierungen über das WAN kopieren zu müssen.

Computer am Standort **Domäne1** empfangen Aktualisierungen und Produktausbringungen direkt vom Master-Repository, das sich auf dem ePolicy Orchestrator-Server befindet (*ePOServer*). Computer, die sich am Standort **Container1** befinden, erhalten diese jedoch von einem verteilten Repository, das auf einem Server liegt.

Die VirusScan Enterprise 8.0i NAP-Datei

Richtlinienseiten oder NAP-Dateien werden zum Konfigurieren der Client-Software über die ePolicy Orchestrator-Konsole verwendet. ePolicy Orchestrator 3.5 wird mit mehreren NAP-Dateien installiert, einschließlich der VirusScan Enterprise 8.0-NAP.

1 Hinzufügen von VirusScan Enterprise zum Master-Repository

Mit den Richtlinienseiten von VirusScan Enterprise 8.0i oder der NAP-Datei können Sie Richtlinien für VirusScan Enterprise 8.0i verwalten, nachdem die Installation auf Client-Computern in Ihrem Netzwerk abgeschlossen ist. Um ePolicy Orchestrator jedoch zum ersten Mal verwenden zu können, *pushen* oder bringen Sie VirusScan Enterprise 8.0i auf die Client-Computer aus, die Sie auch beim VirusScan Enterprise-Ausbringungs- oder Installationspaket in das Master-Software-Repository einchecken müssen. Die Ausbringungspaketdatei heißt `PkgCatalog.z` und ist in der Datei `VSE80iEVAL.ZIP` enthalten, die Sie von der McAfee-Website heruntergeladen haben (siehe hierzu auch *Erhalten der Installationsdateien von McAfee* auf Seite 9).

So checken Sie das VirusScan Enterprise-Paket in Ihr Master-Repository ein:

1. Wählen Sie in der ePolicy Orchestrator-Konsole in der Konsolenstruktur die Option **Repository** aus.
2. Wählen Sie im rechten Detailbereich **Repository** die Option **Paket einchecken** aus.
3. Klicken Sie im Assistenten **Paket einchecken** auf **Weiter**.
4. Wählen Sie auf der zweiten Seite des Assistenten **Produkte oder Aktualisierungen** aus, und klicken Sie auf **Weiter**.

Abbildung 1-5 Assistent: Paket einchecken

5. Wechseln Sie zu dem temporären Ordner mit den VirusScan Enterprise 8.0i-Installationsdateien.
6. Suchen Sie die Paketdatei `PkgCatalog.z` im temporären Ordner von VirusScan Enterprise, und wählen Sie sie aus.
7. Klicken Sie auf **Weiter**, um fortzufahren.

8 Klicken Sie auf der letzten Seite des Assistenten auf **Fertig stellen**, um mit dem Einchecken des Pakets zu beginnen.

Warten Sie, während der ePolicy Orchestrator das Paket in das Repository hochlädt.

Einchecken des Pakets VirusScan 4.5.1 mit Windows 95-, Windows 98- oder Windows Me-Clients

VirusScan Enterprise 8.0i kann nicht auf Windows 95, Windows 98 oder Windows ME ausgeführt werden. Wenn die Clients in Ihrem Testnetzwerk wie in den Beispielen im vorliegenden Handbuch diese Versionen von Windows verwenden, müssen Sie VirusScan 4.5.1. auf diesen Systemen ausbringen. Um dies zu ermöglichen, wiederholen Sie obiges Verfahren, um das Ausbringungspaket VirusScan 4.5.1 in das Software-Repository einzuchecken. Das Paket 4.5.1 wird auch `PkgCatalog.z` genannt und befindet sich in dem temporären Ordner, in den die VirusScan 4.5.1-Installationsdateien extrahiert wurden.

2 Abrufen von Aktualisierungen aus dem McAfee Quell-Repository

Verwenden Sie die HTTP- oder FTP-Site von McAfee als Quell-Repository, von dem aus Sie Ihr Master-Repository mit den neuesten DAT-, Modul- und anderen Dateien aktualisieren können. Starten Sie eine Repository-Abfrage vom Quell-Repository an Ihr Master-Repository, um Folgendes zu tun:

- Testen, ob Ihr ePolicy Orchestrator-Server eine Verbindung zum Quell-Repository über das Internet aufbauen kann
- Aktualisieren des Master-Repositorys mit den neuesten DAT-Dateien

DAT-Dateien werden oft aktualisiert, und die DAT-Dateien, die in Ihren VirusScan Enterprise-Installationsdateien enthalten sind, sind nicht die neuesten. Rufen Sie die neuesten DAT-Dateien vom Quell-Repository ab, bevor Sie VirusScan Enterprise auf Ihrem Netzwerk ausbringen.

Konfigurieren der Proxy-Einstellungen über den Internet Explorer oder in ePolicy Orchestrator

Ihr ePolicy Orchestrator-Server muss auf das Internet zugreifen, um Aktualisierungen vom McAfee Quell-Repository abrufen zu können. Alle anderen Computer in Ihrem Netzwerk benötigen keinen Internetzugang – sie rufen Daten entweder von Ihrem Master-Repository oder von verteilten Repositories auf Ihrem Netzwerk ab (welche im nächsten Schritt eingerichtet werden).

ePolicy Orchestrator verwendet standardmäßig Ihre Proxy-Einstellungen von Internet Explorer. Falls noch nicht geschehen, konfigurieren Sie jetzt Ihre LAN-Verbindung für den Internet Explorer. Wählen Sie die Optionen **Proxy-Server für alle Protokolle verwenden** (FTP und HTTP) und **Proxy für lokale Adressen umgehen** aus.

Alternativ können Sie mit der Option **Proxy-Einstellungen konfigurieren** manuell Proxy-Server-Informationen festlegen. Weitere Informationen hierzu finden Sie im *ePolicy Orchestrator 3.5 Produkthandbuch*.

Starten Sie eine manuelle Abfrage vom McAfee Quell-Repository.

So rufen Sie manuell Aktualisierungen vom Quell-Repository auf Ihr Master-Repository ab:

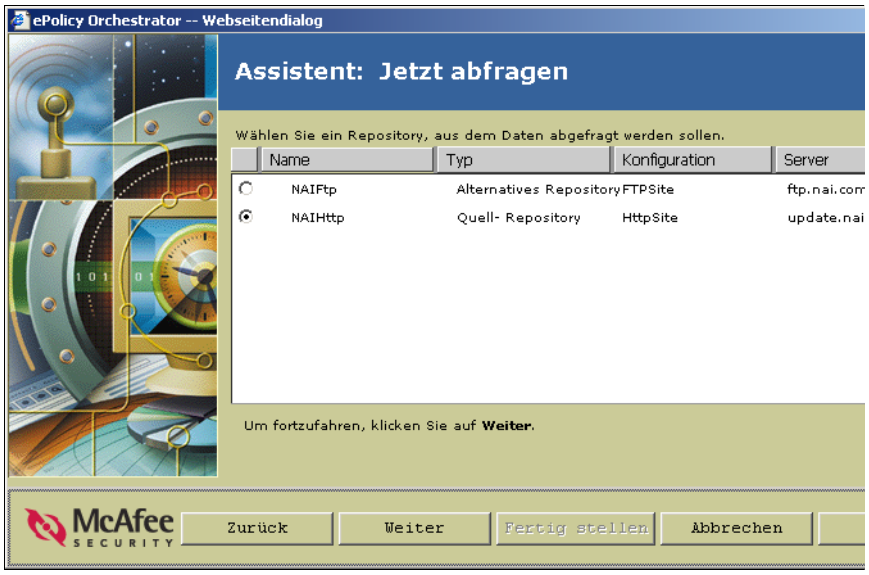
1 Klicken Sie in der Konsolenstruktur auf **Repository**.

2 Wählen Sie im rechten Detailbereich die Optionen **Jetzt abfragen** und **Repository** aus.

3 Klicken Sie im Assistenten **Jetzt abfragen** auf der ersten Seite auf **Weiter**.

4 Wählen Sie auf der nächsten Seite **NAIHttp** aus, und klicken auf **Weiter**. Sie können auch die Standard-**NAIFtp** auswählen, HTTP ist in der Regel jedoch zuverlässiger.

Abbildung 1-6 Assistent: Jetzt abrufen



5 Vergewissern Sie sich beim Verwalten von älteren Produkten (z. B. VirusScan 4.5.1 für Computer unter Windows 95 oder Windows 98), dass **Legacy-Produktaktualisierung** ausgewählt ist.

6 Klicken Sie auf der letzten Seite auf **Fertig stellen**, um alle Standardeinstellungen auf dieser Seite zu übernehmen und mit dem Abrufen zu beginnen.

Warten Sie einige Minuten, während der Pull-Task ausgeführt wird.

7 Klicken Sie auf **Schließen**, wenn das Abrufen beendet ist.

Jetzt haben Sie VirusScan Enterprise in Ihr Master-Repository eingecheckt und das Master-Repository mit den neuesten DAT- und Moduldateien vom McAfee Quell-Repository aktualisiert. Die Computer, die sich in derselben Domäne befinden wie Ihr ePolicy Orchestrator-Server (in diesem Beispiel die Computer am Standort **Domäne1** im **Verzeichnis**), rufen VirusScan Enterprise vom Master-Repository ab.

Wo rufen andere Computer ihre Software und Aktualisierungen ab? Wenn sich diese Computer in unterschiedlichen Subnets oder einem über WAN angeschlossenen Speicherort befinden, ist es möglicherweise effizienter, ein verteiltes Repository oder eine Kopie des Master-Repositorys zu erstellen, die für diese Computer leichter zugänglich ist.

3 Erstellen eines verteilten Repositories

Nun muss ein verteiltes Repository in **Container1** erstellt werden, damit Aktualisierungen für diese Computer von dort durchgeführt werden können. Ihr Testnetzwerk ist mit nur wenigen Clients und einem ePolicy Orchestrator-Server so klein, dass keine ausgefeilte Struktur der verteilten Repositories benötigt wird. Sie können die Beispiele zu verteilten Repositories in diesem Handbuch jedoch verwenden, um reale Szenarien zu simulieren. Ein solches Szenario könnte Computer in Remote-Domänen beinhalten, die auf dem ePolicy Orchestrator-Server nicht effizient über ein Master-Repository, das über WAN angeschlossen ist, aktualisiert werden können.

Sie können FTP, HTTP oder UNC verwenden, um Daten vom Master-Repository auf die verteilten Repositories zu replizieren. In diesem Handbuch wird beschrieben, wie ein verteiltes Repository, das sich auf einer UNC-Freigabe befindet, auf einem der Computer am Standort **Container1** erstellt wird.

Führen Sie dazu folgende Schritte aus:

1 *Erstellen eines gemeinsam genutzten Ordners auf einem Computer als Repository*.

2 *Hinzufügen des verteilten Repositorys zum ePolicy Orchestrator-Server*.

3 *Replizieren von Daten vom Master-Repository auf die verteilten Repositories*.

4 *Konfigurieren der Remote-Site für das verteilte Repository*.

1 Erstellen eines gemeinsam genutzten Ordners auf einem Computer als Repository

Bevor Sie das über UNC verteilte Repository zu ePolicy Orchestrator hinzufügen, müssen Sie zunächst den zu verwendenden Ordner erstellen. Zusätzlich müssen Sie den Ordner auf Freigabe im gesamten Netzwerk einstellen, so dass der ePolicy Orchestrator-Server Dateien in diesen Ordner kopieren kann.

So erstellen Sie einen gemeinsam genutzten Ordner für ein über UNC verteiltes Repository:

1 Erstellen Sie auf dem Computer, der als Host für das verteilte Repository dienen soll, im Windows Explorer einen neuen Ordner.

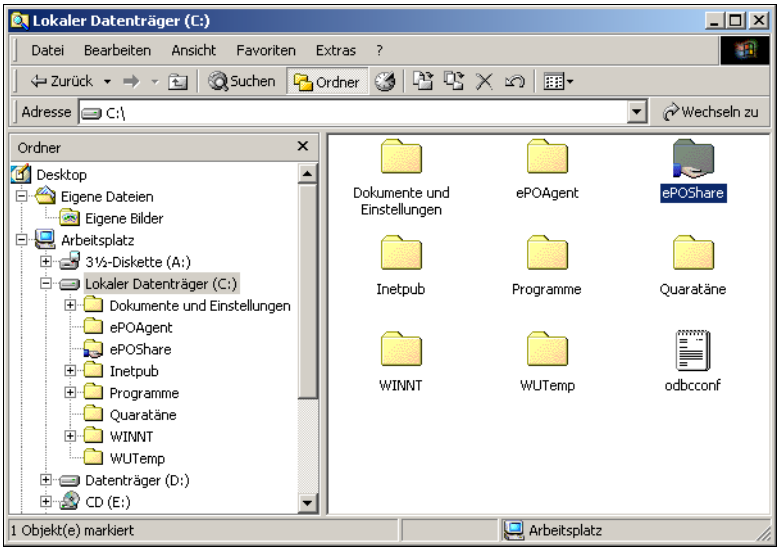
2 Klicken Sie mit der rechten Maustaste auf den Ordner, und wählen Sie **Freigabe** aus.

3 Wählen Sie auf der Registerkarte **Freigabe** die Option **Diesen Ordner freigeben** aus.

4 Klicken Sie auf **OK**, um alle anderen Standardeinstellungen zu übernehmen und die Ordnerfreigabe zu aktivieren.

Das Erstellen einer UNC-Freigabe auf diese Art und Weise stellt in einer Produktionsumgebung ein potenzielles Sicherheitsrisiko dar, da es jedem Teilnehmer in Ihrem Netzwerk Zugriff auf die Freigabe ermöglicht. Wenden Sie gegebenenfalls zusätzliche Sicherheitsmaßnahmen an, um den Zugriff auf den gemeinsam genutzten Ordner zu kontrollieren, wenn sie einen UNC-Ordner in einer Produktionsumgebung erstellen oder nicht wissen, ob Ihre Netzwerktestumgebung sicher ist. Client-Computer erfordern nur Lesezugriff, um Aktualisierungen vom UNC-Repository abzurufen. Administrator-Benutzerkonten, einschließlich dem Konto, das vom ePolicy Orchestrator zur Datenreplikation verwendet wird, erfordern jedoch auch Schreibzugriff. Informationen zum Konfigurieren der Sicherheitseinstellungen für gemeinsam genutzte Ordner finden Sie in der Microsoft Windows-Dokumentation.

Abbildung 1-7 Microsoft Explorer



2 Hinzufügen des verteilten Repositorys zum ePolicy Orchestrator-Server

Wenn Sie den als UNC-Freigabe zu verwendenden Ordner erstellt haben, fügen Sie ein verteiltes Repository zum Repository von ePolicy Orchestrator hinzu und weisen es dem erstellten Ordner zu.

So fügen Sie das verteilte Repository hinzu:

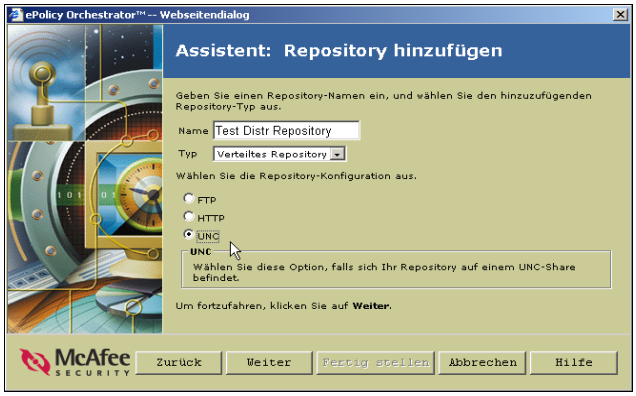
1 Klicken Sie in der Konsolenstruktur auf **Repository**.

2 Wählen Sie im Detailbereich **Repository** die Option **Verteiltes Repository hinzufügen** aus.

3 Klicken Sie auf der ersten Seite des Assistenten auf **Weiter**.

4 Geben Sie im Feld **Name** einen Namen ein. Beachten Sie, dass das verteilte Repository unter diesem Namen in der Repository-Liste in der ePolicy Orchestrator-Konsole angezeigt wird. Es muss sich dabei nicht um den speziellen Namen des Freigabeordners handeln, der tatsächlich als Host für das Repository dient.

Abbildung 1-8 Assistent: Repository hinzufügen



5 Wählen Sie in der Dropdown-Liste **Typ** die Option **Verteiltes Repository** aus.

6 Wählen Sie **UNC** für die Konfiguration des Repositorys aus, und klicken Sie auf **Weiter**.

7 Geben Sie den Pfad des gemeinsam genutzten Ordners an, den Sie erstellt haben. Geben Sie einen gültigen UNC-Pfad an. In diesem Handbuch gibt es folgendes Beispiel: `\\BU06\ePOShare`, wobei `BU06` der Name eines Computers in **Container1** und `ePOShare` der Name eines freigegebenen UNC-Ordners ist.

8 Klicken Sie auf **Weiter**.

9 Deaktivieren Sie auf der Seite der **Anmeldeinformationen zum Herunterladen** die Option **Angemeldetes Konto verwenden**.

10 Geben Sie Informationen wie die entsprechende Domäne, den Benutzernamen und das Kennwort an, die die Client-Computer verwenden sollten, wenn sie Aktualisierungen von diesem verteilten Repository herunterladen.

11 Klicken Sie auf **Prüfen**, um die Anmeldeinformationen zu testen. Nach wenigen Sekunden sollte ein Bestätigungsdialogfeld angezeigt werden, in dem bestätigt wird, dass die Freigabe für Clients zugänglich ist.

Abbildung 1-9 Bestätigungsdialogfeld

Wenn Ihr Standort nicht bestätigt wurde, überprüfen Sie, ob Sie den UNC-Pfad auf der vorherigen Seite des Assistenten korrekt eingegeben und die Freigabe für den Ordner korrekt konfiguriert haben.

12 Klicken Sie auf **Weiter**.

13 Geben Sie Anmeldeinformationen zum Replizieren ein, indem Sie Domäne, Benutzernamen und Kennwort in die entsprechenden Textfelder eingeben.

Der ePolicy Orchestrator-Server verwendet diese Anmeldeinformationen beim Kopieren oder Replizieren von DAT-Dateien, Moduldateien oder anderen Produktaktualisierungen vom Master-Repository auf das verteilte Repository. Diese Anmeldeinformationen müssen in der Domäne, in der sich das verteilte Repository befindet, über Administratorrechte verfügen. In unseren Beispielen können dieselben Anmeldeinformationen verwendet werden, die auch für die Ausbringung des Agenten verwendet werden. Weitere Informationen hierzu finden Sie unter *Starten einer Agenteninstallation auf den Computern an Ihrem Standort* auf Seite 22.

14 Klicken Sie auf **Prüfen**, um zu überprüfen, ob Ihr ePolicy Orchestrator-Server in den freigegebenen Ordner auf dem Remote-Computer schreiben kann. Nach wenigen Sekunden sollten Sie ein Bestätigungsdialogfeld sehen, in dem dies bestätigt wird.

15 Klicken Sie auf **Fertig stellen**, um das Repository hinzuzufügen. Warten Sie einen Moment, während ePolicy Orchestrator das neue verteilte Repository zu seiner Datenbank hinzufügt.

16 Klicken Sie auf **Schließen**.

3 Replizieren von Daten vom Master-Repository auf die verteilten Repositories

Jetzt haben Sie eine UNC-Freigabe auf einem Computer als Host für das verteilte Repository erstellt und Ihrer ePolicy Orchestrator-Datenbank den Repository-Speicherort hinzugefügt. Es fehlen nun lediglich die Daten im neuen Repository. Wenn Sie den erstellten Freigabeordner durchsuchen, stellen Sie fest, dass dieser noch leer ist.

Verwenden Sie die Funktion **Jetzt replizieren**, um Ihre verteilten Repositories manuell mit den neuesten Inhalten Ihres Master-Repositorys zu aktualisieren. Später wird ein Replikations-Task geplant, damit dies automatisch geschieht.

So starten Sie manuell eine Replikation:

1 Klicken Sie in der Konsolenstruktur auf **Repository**.

2 Klicken Sie auf der Seite **Repository** auf **Jetzt replizieren**, um den Assistenten **Jetzt replizieren** anzuzeigen.

3 Klicken Sie auf der ersten Seite des Assistenten auf **Weiter**.

4 Wählen Sie in der Liste der verfügbaren Repositories das von Ihnen erstellte verteilte Repository aus, und klicken Sie auf **Weiter**.

5 Wählen Sie **Inkrementelle Replikation** aus.

Da dies ein neues verteiltes Repository ist und Sie zum ersten Mal auf dieses replizieren, können Sie auch **Vollständige Replikation** auswählen. Für zukünftige Replizierungen sollten Sie jedoch eine inkrementelle Replizierung ausführen, um Zeit und Bandbreite einzusparen.

6 Klicken Sie auf **Fertig stellen**, um die Replizierung zu starten. Warten Sie einige Minuten, während die Replikation abgeschlossen wird.

7 Klicken Sie auf **Schließen**, um das Fenster des Assistenten zu schließen.

Wenn Sie jetzt zu Ihrem Ordner `ePOShare` gehen, werden Sie feststellen, dass er Unterordner für Agenten und Software enthält.

4 Konfigurieren der Remote-Site für das verteilte Repository

Nachdem Sie das verteilte Repository erstellt haben, können Sie es nun verwenden. Wie bereits erwähnt, ist Ihr Testnetzwerk zu klein, als dass die verteilten Repositories tatsächlich benötigt würden. Um jedoch die Arbeitsweise der verteilten Repositories zu simulieren, kann die Aktualisierung so konfiguriert werden, dass Computer an einem Standort Ihres **Verzeichnisses** Aktualisierungen nur vom verteilten und nicht vom Master-Repository durchführen.

Um dies in Ihrem Test zu simulieren, werden die Agentenrichtlinien für einen der Standorte in Ihrem **Verzeichnis** so konfiguriert, dass nur das neue verteilte Repository verwendet wird. In unserem Beispielnetzwerk in diesem Handbuch ist dies der Standort **Container1**, auf dem sich der Win2KServer-Computer als Host für Ihr neu erstelltes verteiltes Repository befindet.

So konfigurieren Sie die ePolicy Orchestrator-Agentenrichtlinie für den Standort **Container1** für die Verwendung des verteilten Repositorys zum Aktualisieren:

1 Wählen Sie im **Verzeichnis** in der Konsolenstruktur den Standort aus, den das verteilte Repository verwenden soll.

2 Klicken Sie im rechten Richtlinienbereich auf die Registerkarte **Richtlinien**.

3 Erweitern Sie den **ePolicy Orchestrator-Agenten**, und wählen Sie die Option **Konfiguration** aus.

4 Klicken Sie auf die Registerkarte **Repositories** der ePolicy Orchestrator-Agentenrichtlinie.

5 Deaktivieren Sie die Option **Vererben**, um die Repository-Optionen zu aktivieren.

6 Wählen Sie unter **Repository-Auswahl** die **Benutzerdefinierte Liste** aus.

7 Deaktivieren Sie in der **Repository-Liste** alle Repositories, bis nur noch Ihr verteiltes Repository aktiviert ist.

8 Klicken Sie im oberen Bereich der Seite auf **Alle übernehmen**, um die Änderungen zu speichern.

Wenn bei den Computern auf diesem Standort Aktualisierungen erforderlich sind, werden diese vom verteilten Repository abgerufen.

Das Erzwingen von Aktualisierungen von bestimmten Repositories wird hier, wie bereits erwähnt, nur zum Zweck der Simulation verteilter Repositories in einem Labornetzwerk dargestellt. In einer Produktionsumgebung würde man dagegen anders verfahren. Hier wären zusätzliche Tasks für Fail-Over erforderlich. Aufgrund schnellerer Netzwerkverbindungen würden Client-Computer eher über ein lokales verteiltes Repository aktualisieren als über WAN auf das Master-Repository, auch wenn dies nicht speziell konfiguriert wurde. Andererseits könnte der Client immer noch von anderen Repositories auf dem Netzwerk aktualisieren, wenn das verteilte Repository aus irgendeinem Grund nicht verfügbar wäre.

SCHRITT 5

Festlegen von VirusScan Enterprise 8.0i-Richtlinien vor der Ausbringung

Nachdem Sie die Repositories erstellt und ihnen das VirusScan Enterprise-Ausbringungspaket hinzugefügt haben, können Sie fast VirusScan Enterprise auf Ihre Clients ausbringen. Vor dem Ausbringen von VirusScan Enterprise werden jedoch die Richtlinien geringfügig geändert. Hier kommt die NAP-Datei zum Einsatz, die Sie eingecheckt haben. Sie können diese zur Konfiguration der VirusScan Enterprise-Funktionen verwenden, sobald die Installation auf dem Client-Computer abgeschlossen ist. Folgendes Beispiel veranschaulicht die Vorgehensweise: Ändern der Richtlinien für Workstations, um VirusScan Enterprise 8.0i mit eingeschränkter Benutzeroberfläche zu installieren. Server behalten die Standardrichtlinie bei, mit der die vollständige Benutzeroberfläche angezeigt wird.

Dies könnte eine potenziell nützliche Implementierung in Ihrem tatsächlichen Netzwerk sein, in dem Sie die Taskleiste-Benutzeroberfläche auf Ihrer Workstation möglicherweise ausblenden möchten, um so zu verhindern, dass Endbenutzer Ihre Richtlinien einfach ändern oder bestimmte Funktionen deaktivieren können.

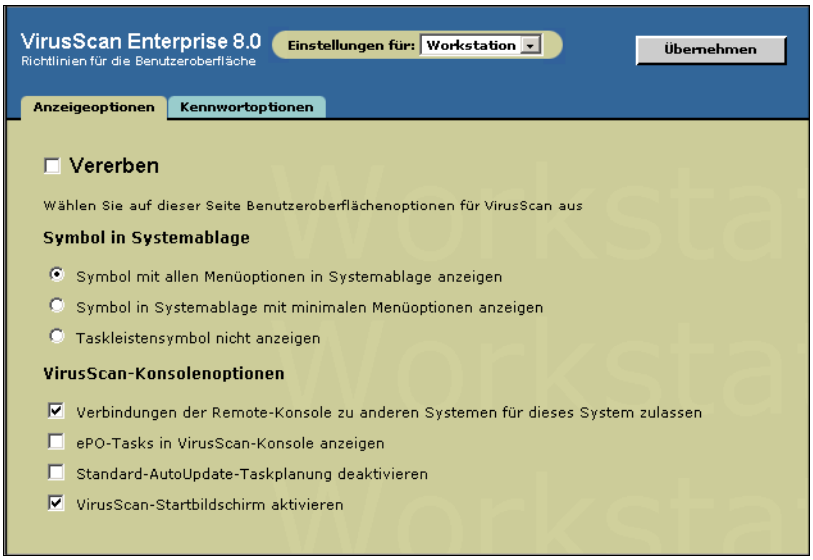
Um diese Richtlinien festzulegen, werden die **Workstation**-Gruppen verwendet, die beim Verfassen Ihres **Verzeichnisses** erstellt wurden. Sie können die Richtlinien jeweils einmal für jede Workstation-Gruppe ändern (innerhalb von **Domäne1** und **Container1**), damit diese an alle Computer innerhalb dieser Gruppen vererbt werden. Für Server kann die Standardrichtlinie beibehalten werden, die VirusScan Enterprise mit den vollständigen, in der Taskleiste verfügbaren, Menüoptionen installiert.

So ändern Sie die VirusScan Enterprise-Richtlinien für Workstations:

1. Klicken Sie in der Konsolenstruktur auf Ihre *Workstation*-Gruppe in einem Standort.
2. Klicken Sie im Detailbereich auf die Registerkarte **Richtlinien**, und wählen Sie **VirusScan Enterprise 8.0i** aus.

3 Wählen Sie **Benutzeroberflächen-Richtlinien** aus.

Abbildung 1-10 Benutzeroberflächen-Richtlinien



4 Wählen Sie oben auf der Seite in der Dropdown-Liste unter **Einstellungen für** die Option **Workstation**.

Mit der Dropdown-Liste **Einstellungen für** können Sie separate Richtlinien für Server und Workstations festlegen, ohne dabei **Verzeichnis**-Gruppen zu verwenden. ePolicy Orchestrator erkennt das Betriebssystem auf dem Client-Computer und übernimmt die richtige Richtlinie. Zu Testzwecken kann es jedoch nützlich sein, Gruppen von Servern und Workstations zu erstellen.

5 Deaktivieren Sie **Vererben**, damit die Optionen der Benutzeroberflächen-Richtlinien verfügbar werden.

6 Wählen Sie **Symbol in Systemablage mit minimalen Menüoptionen anzeigen** aus.

7 Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

8 Wiederholen Sie diese Schritte für weitere *Workstation*-Gruppen in Ihrem **Verzeichnis**.

SCHRITT

6

Ausbringen von VirusScan Enterprise auf Clients

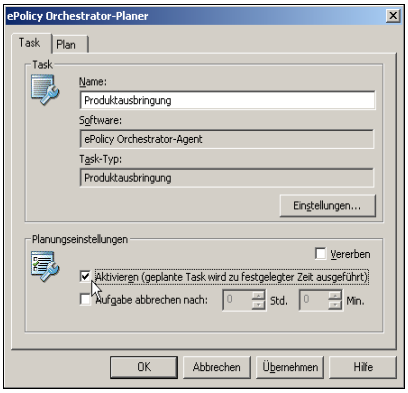
Nun haben Sie Master- und verteilte Repositories erstellt, die VirusScan Enterprise 8.0i PKGCATALOG.Z-Datei Ihrem Master-Repository hinzugefügt und dies auf ein neues verteiltes Repository repliziert. Ihre Computer werden zum **Verzeichnis** hinzugefügt. Auf allen Computern sind ePolicy Orchestrator-Agenten installiert. Sie haben Ihre VirusScan Enterprise-Richtlinien für Server und Workstations definiert. Nun kann ePolicy Orchestrator auf allen Clients in Ihrem Testnetzwerk VirusScan Enterprise ausbringen.

Im Gegensatz zum Ausbringen von Agenten, was auf Standort-, Gruppen- oder Computerebene ausgeführt werden muss, können Sie VirusScan Enterprise auf **Verzeichnisebene** ausbringen, um es auf allen Computern in dem **Verzeichnis** gleichzeitig zu installieren. Beachten Sie, dass alle Richtlinien, die Sie für bestimmte Standorte oder Gruppen innerhalb Ihres **Verzeichnisses** übernommen haben (in diesem Beispiel **Server** und **Workstation**-Gruppen), auch dann gelten, wenn VirusScan Enterprise auf Clients innerhalb dieser Gruppen installiert wird. Alternativ können Sie VirusScan Enterprise auf Standorten, Gruppen oder einzelnen Computern ausbringen. Die in diesem Abschnitt beschriebenen Schritte können Sie auf jeder Ebene in Ihrem **Verzeichnis** zum Ausbringen verwenden.

So bringen Sie VirusScan Enterprise 8.0i auf allen Computern in Ihrem **Verzeichnis** aus:

1. Wählen Sie in der Konsolenstruktur **Verzeichnis** aus.
2. Wählen Sie im Detailbereich die Registerkarte **Task** aus, und doppelklicken Sie anschließend in der Taskliste auf den Task **Produktausbringung**.
3. Wenn der **ePolicy Orchestrator-Planer** geöffnet wird, klicken Sie auf die Registerkarte **Task**, und deaktivieren Sie **Vererben** unter **Planungseinstellungen**.

Abbildung 1-11 Dialogfeld "ePolicy Orchestrator-Planer"



4. Wählen Sie im Bereich **Planungseinstellungen** die Option **Aktivieren (geplante Task wird zu festgelegter Zeit ausgeführt)** aus.
5. Klicken Sie auf die Schaltfläche **Einstellungen**.
6. Deaktivieren Sie auf der Seite **Produktausbringung** die Option **Vererben**, damit die Optionen für die Produktausbringung verfügbar werden.
7. Legen Sie als **Aktion** für den **VirusScan Enterprise 8.0i**-Ausbringungs-Task **Installieren** fest.

8 Klicken Sie auf **OK**, um die Optionen für die Produktausbringung zu speichern und zum Dialogfeld **ePolicy Orchestrator-Planer** zurückzukehren.

9 Klicken Sie im Dialogfeld **ePolicy Orchestrator-Planer** auf die Registerkarte **Plan**.

10 Deaktivieren Sie **Vererben**, damit die Planungsoptionen verfügbar werden.

11 Wählen Sie in der Dropdown-Liste **Task planen** die Option **Sofort ausführen** aus.

12 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

In der Taskliste auf der Registerkarte **Tasks** des Detailbereichs wird der Status **Aktiviert** für den Ausbringungs-Task auf **Ja** gesetzt.

Jetzt haben Sie Ihren standardmäßigen Ausbringungs-Task konfiguriert und können VirusScan Enterprise auf allen Client-Computern an ihrem Teststandort installieren. Die Ausbringung wird ausgeführt, wenn die Agenten das nächste Mal aktualisierte Anweisungen vom ePolicy Orchestrator-Server abrufen. Sie können auch eine Agenten-Reaktivierung initiieren, damit die Ausbringung sofort ausgeführt wird. Weitere Informationen hierzu finden Sie unter *Senden einer Agentenreaktivierung, um die sofortige Rückmeldung zu erzwingen* auf Seite 38.

Ausbringen von VirusScan 4.5.1 auf Computer mit Windows 95, Windows 98 oder Windows Me

Falls Sie wie in diesem Beispiel Computer mit Windows 95, 98 oder Windows Me in Ihrem Testnetzwerk haben, können Sie die Schritte in diesem Abschnitt wiederholen, um nur VirusScan 4.5.1 auf diesen Computern auszubringen. Vergewissern Sie sich, dass Sie das Ausbringungspaket VirusScan 4.5.1 in das Repository eingecheckt haben (siehe hierzu *Einchecken des Pakets VirusScan 4.5.1 mit Windows 95-, Windows 98- oder Windows Me-Clients* auf Seite 27). Das Ausbringen von VirusScan 4.5.1 auf mehreren Computern ist am einfachsten, wenn Sie Ihre Computer mit Windows 95, 98 oder Me in einer Gruppe in Ihrem **Verzeichnis** organisiert haben. Sie können den Ausbringungs-Task jedoch auch für einzelne Computer ausführen.

So bringen Sie VirusScan 4.5.1 aus:

1 Wählen Sie in der Konsolenstruktur Ihre Gruppe oder Ihren Computer im **Verzeichnis** aus.

2 Klicken Sie im Detailbereich auf die Registerkarte **Tasks**. Befolgen Sie die Schritte im vorherigen Abschnitt, um die Ausbringung wie für VirusScan Enterprise 8.0i zu konfigurieren.

3 Legen Sie auf der Seite mit den **Ausbringungseinstellungen** für VirusScan 4.5.1 **Installieren** fest.

   Sie können VirusScan Enterprise 8.0i auf **Ignorieren** einstellen, dies ist aber nicht erforderlich. VirusScan Enterprise erkennt, dass auf diesen Computern eine frühere Version von Windows ausgeführt und installiert nicht.

4 Führen Sie die Schritte zur Ausbringungskonfiguration aus. ePolicy Orchestrator bringt VirusScan 4.5.1 aus, wenn sich die Agenten auf diesen Computern das nächste Mal beim Server zurückmelden.

Senden einer Agentenreaktivierung, um die sofortige Rückmeldung zu erzwingen

Falls erwünscht können Sie die Agenten sofort reaktivieren. Dies veranlasst die Agenten, sofort mit dem ePolicy Orchestrator-Server einzuchecken, anstatt auf die nächste geplante Rückmeldung der Agenten zu warten, die standardmäßig auf 60 Minuten festgelegt ist. Wenn sich der Agent zurückmeldet, sehen sie, dass die VirusScan Enterprise-Ausbringung so eingestellt ist, dass installiert und nicht ignoriert wird. Anschließend rufen die Agenten die VirusScan Enterprise `PkgCatalog.z`-Datei vom Repository ab und installieren VirusScan Enterprise. Beachten Sie, dass jeder Agent die `PkgCatalog.z`-Datei vom jeweiligen konfigurierten Repository abruft. In unserem Beispielnetzwerk rufen die Computer am Standort **Domäne1** vom Master-Repository und die Computer von **Container1** vom neu erstellten verteilten Repository ab.

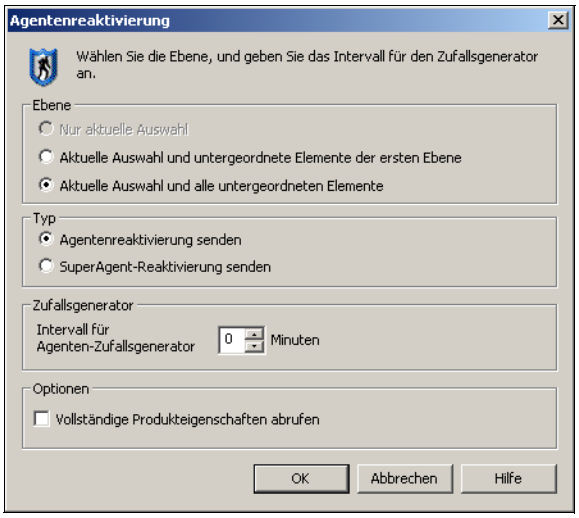
Sie können an alle Standorte, Gruppen oder einzelne Computer im **Verzeichnis** eine Agentenreaktivierung senden. Da alle Computer im **Verzeichnis** reaktiviert werden sollen, wird für alle Standorte eine Reaktivierung initiiert, die diese an Gruppen und Computer auf diesem Standort vererben.

So senden Sie eine Agentenreaktivierung, um sofort mit der Ausbringung von VirusScan Enterprise zu beginnen:

1 Klicken Sie mit der rechten Maustaste auf den Zielstandort in der **Konsolenstruktur**, und wählen Sie **Agentenreaktivierung** aus.

2 Legen Sie den **Intervall für Agenten-Zufallsgenerator** auf **0** Minuten fest.

Abbildung 1-12 Dialogfeld "Agentenreaktivierung"



3 Klicken Sie auf **OK**, um alle anderen Standardeinstellungen zu übernehmen und die Reaktivierung zu senden.

4 Wiederholen Sie diese Schritte für andere Standorte in Ihrem **Verzeichnis**.

Die Agenten melden sich sofort zurück, rufen die Richtlinienänderungen für die Ausbringung ab und beginnen mit der Installation von VirusScan Enterprise. Warten Sie einige Minuten, bis VirusScan Enterprise 8.0i ausgebracht und installiert ist.

Sie können auf mehrere Arten überprüfen, ob die Installation auf mehreren Clients erfolgreich verlaufen ist. Überprüfen Sie auf dem Client-Computer, ob Folgendes ausgeführt wurde:

- Der `MCSHIELD.EXE`-Prozess läuft und wird auf der Registerkarte **Prozesse** des **Windows Task-Managers** angezeigt.
- Ein VirusScan-Ordner wurde dem Ordner `Programme/Network Associates` hinzugefügt.
- Wenn Sie die Richtlinie, diesen auszublenden, nicht geändert haben, wird das VShield-Symbol in der Taskleiste neben dem Agentensymbol angezeigt. Möglicherweise ist ein Neustart erforderlich, um das Taskleistensymbol anzuzeigen. Beachten Sie, dass VirusScan aktiv ist und läuft, auch wenn das VShield-Symbol noch nicht in der Taskleiste angezeigt wurde.

SCHRITT 7

Ausführen einen Berichts, um den Schutzumfang zu bestätigen

Eine andere Möglichkeit für die Bestätigung einer erfolgreichen VirusScan Enterprise-Ausbringung bietet die Verwendung eines der Berichte, die in ePolicy Orchestrator enthalten sind. Führen Sie einen *Übersicht "Produktschutz"*-Bericht aus, um zu bestätigen, dass die VirusScan Enterprise-Ausbringung erfolgreich war. Beachten Sie, dass es unter Umständen eine Stunde dauert, bis die Datenbank auf den neuesten Stand aktualisiert wurde.

So führen Sie einen *Übersicht "Produktschutz"*-Bericht aus:

1. Wählen Sie im linken Bereich der Konsolenstruktur **Berichterstellung** | **ePO-Datenbanken** | **ePO_ePOServer** aus. ePOServer steht für den Namen der in diesem Beispiel verwendeten ePolicy Orchestrator-Datenbank.
2. Wenn Sie aufgefordert werden, sich bei der Datenbank anzumelden, geben Sie Ihre MSDE-Anmeldeinformationen für `sa` ein, die Sie beim Installieren der Konsole und Datenbank erstellt haben.
3. Wählen Sie **Berichte** | **Antivirus** | **Deckung** | **Übersicht "Produktschutz"** aus.
4. Wählen Sie **Nein** aus, wenn Sie aufgefordert werden, einen Datenfilter festzulegen. Gedulden Sie sich einen Moment, während ePolicy Orchestrator den Bericht erstellt.

Nach der Erstellung des Berichts sollten die Ergebnisse die Anzahl an Servern und Workstations anzeigen, auf denen VirusScan 4.5.1 und VirusScan Enterprise 8.0i derzeit installiert sind. Wenn Sie später andere Produkte (z. B. McAfee Desktop Firewall) ausbringen, werden sie in diesem Bericht ebenfalls angezeigt. In unserem Beispiel können Sie erkennen, dass VirusScan Enterprise 8.0i und VirusScan 4.5.1 auf allen Computern in unserem Testnetzwerk installiert wurden.

SCHRITT

8

Aktualisieren von DAT-Dateien mit einer geplanten Client-Aktualisierung

Am häufigsten werden Sie mit dem ePolicy Orchestrator DAT-Virusdefinitionsdateien aktualisieren. VirusScan Enterprise führt standardmäßig sofort nach der Installation einen Aktualisierungs-Task durch. Wenn Sie die Schritte zur Konfiguration Ihrer Repositories in diesem Handbuch befolgt haben und die neuesten DAT-Dateien vor dem Ausbringen auf Ihr Master-Repository abgerufen haben, ist VirusScan Enterprise kurz nach der Ausbringung auf dem aktuellsten Stand.

Nachdem VirusScan Enterprise installiert ist, sollten Sie die DAT-Dateien jedoch regelmäßig aktualisieren. Ihre Virenschutzsoftware ist nur so gut wie dessen neueste DAT-Dateien, daher ist es besonders wichtig, diese auf dem aktuellsten Stand zu halten. In einem späteren Abschnitt in diesem Handbuch wird behandelt, wie regelmäßige automatische Client-Aktualisierungs-Tasks festgelegt werden, die beispielsweise täglich oder wöchentlich stattfinden sollen. Wenn Sie eine sofortige DAT-Dateiaktualisierung initiieren möchten, werden Sie dazu wahrscheinlich zu einem bestimmten Zeitpunkt aufgefordert, beispielsweise wenn McAfee als Antwort auf einen neu entdeckten Virus aktualisierte DAT-Dateien veröffentlicht und Sie möchten, dass Ihre Clients aktualisieren, ohne dass sie auf ihren regelmäßig festgelegten Task warten.

Erstellen dazu einen Client-Aktualisierungs-Task, und führen Sie ihn von Ihrer ePolicy Orchestrator-Konsole aus. Dies veranlasst Ihre gesamte Client-Antivirensoftware dazu, einen Aktualisierungs-Task durchzuführen.

Stellen Sie vor dem Ausführen eines Client-Aktualisierungs-Tasks sicher, dass Sie zuerst alle aktualisierten DAT- oder Moduldateien in Ihr Master-Repository und Ihre verteilten Repositories laden, falls vorhanden. Weitere Informationen hierzu finden Sie unter *Einrichten des Master-Repositorys und anderen verteilten Repositories* auf Seite 25.

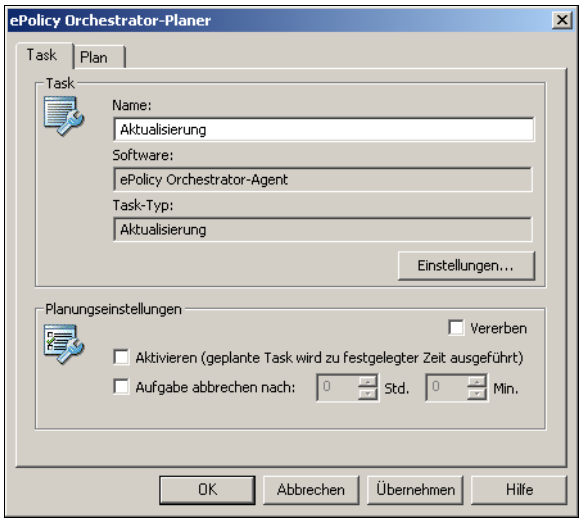
So erstellen Sie einen Client-Aktualisierungs-Task und führen ihn aus:

1. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf das **Verzeichnis**, und wählen Sie **Task planen** aus.
2. Geben Sie im Dialogfeld **Task planen** einen Namen in das Feld **Name der neuen Task** ein, z. B. **Client-DATs aktualisieren**.
3. Wählen Sie in der Softwareliste **ePolicy Orchestrator Agent | Aktualisierung** für den Tasktyp aus.
4. Klicken Sie auf **OK**.
5. Drücken Sie **F5**, um die Konsole zu aktualisieren. Der neue Task wird anschließend auf der Registerkarte **Task** in der Liste angezeigt.

   Beachten Sie, dass seine Ausführung täglich zur momentan eingestellten Zeit geplant wird. Beachten Sie auch, dass das **Aktiviert**-Flag auf **Nein** eingestellt ist. Dies muss nun in **Ja** geändert und sofort ausgeführt werden.
6. Klicken Sie mit der rechten Maustaste auf den neuen Task in der Liste, und wählen Sie **Task bearbeiten** aus.

7 Deaktivieren Sie **Vererben** im Abschnitt **Planungseinstellungen** des Dialogfeldes **ePolicy Orchestrator-Planer**.

Abbildung 1-13 Dialogfeld "ePolicy Orchestrator-Planer"



8 Wählen Sie **Aktivieren** aus.

9 Klicken Sie auf **Einstellungen**, und deaktivieren Sie **Vererben** auf der Registerkarte **Aktualisierung**.

10 Stellen Sie sicher, dass die Option **Dieser Task aktualisiert nur folgende Komponenten** ausgewählt ist. Hiermit können Sie festlegen, welche Komponenten Sie aktualisieren möchten. Dadurch können Netzwerkressourcen einsparen, indem Sie die Anzahl der Aktualisierungen in Ihrer Umgebung begrenzen.

11 Belassen Sie die Standardeinstellungen unter **Signaturen und Module**.

12 Wählen Sie unter **Patches und Service Packs** die Option **VirusScan Enterprise 8.0** aus, und klicken Sie anschließend auf **OK**.

13 Klicken Sie auf die Registerkarte **Plan**, und deaktivieren Sie die Option **Vererben**.

14 Legen Sie für **Task planen** die Option **Sofort ausführen** fest, und klicken Sie auf **OK**.

15 Initiieren Sie die Agentenreaktivierung auf allen Standorten in Ihrem **Verzeichnis**, damit Ihre Agenten sich sofort melden, um den Agenten-Aktualisierungs-Task abzurufen. Weitere Informationen hierzu finden Sie unter *Senden einer Agentenreaktivierung, um die sofortige Rückmeldung zu erzwingen* auf Seite 38.

Woran kann ich erkennen, dass VirusScan Enterprise auf die neuesten DATs aktualisiert hat?

Überprüfen Sie, welche DAT-Version derzeit im Master-Repository eingecheckt ist. Das sind die DATs, die sich nun auf den Client-Computern befinden sollten, nachdem sie aktualisiert worden sind. Führen Sie dazu folgende Schritte aus:

1. Wählen Sie in der Konsolenstruktur **Repository** | **Software-Repositories** | **Master** aus. Im Detailbereich wird eine Liste der momentan im Master-Repository eingecheckten Pakete angezeigt.
2. Führen Sie einen Bildlauf zum Ende der Liste **Pakete** aus, und suchen Sie nach **Aktuelle DAT-Version**, was eine 4-ziffrige Nummer wie **4306** sein wird.

Überprüfen Sie als Nächstes über die ePolicy Orchestrator-Konsole, welche DAT-Versionen die Client-Software verwendet, z. B. VirusScan Enterprise. Beachten Sie, dass auf der Konsole erst dann der aktualisierte Status angezeigt wird, wenn der Agent das nächste Mal im Rahmen der Agent-zu-Server-Kommunikation einen Aufruf an den Server sendet. Führen Sie dazu folgende Schritte aus:

1. Wählen Sie auf der ePolicy Orchestrator-Konsole im **Verzeichnis** einen beliebigen kürzlich aktualisierten Computer aus.
2. Wählen Sie im Detailbereich die Registerkarte **Eigenschaften** aus.
3. Wählen Sie auf der Seite **Eigenschaften** die Optionen **VirusScan Enterprise 8.0i** | **Allgemein** aus, um die Liste mit allgemeinen Eigenschaften zu erweitern.
4. Überprüfen Sie die Nummer der **DAT-Version**. Sie sollte der aktuellsten DAT-Version im Master-Software-Repository entsprechen.

SCHRITT 9

Planen der automatischen Repository-Synchronisierung

Sie sind nun schon weit gekommen. In einigen Stunden haben Sie eine voll funktionsfähige Installation von ePolicy Orchestrator in Ihrem Testnetzwerk ausgebracht. Die Agenten bringen auf Client-Computern aus, und diese Agenten sind aktiv und rufen regelmäßig aktualisierte Anweisungen vom Server ab. Sie haben ePolicy Orchestrator verwendet, um VirusScan Enterprise auf Ihren Client-Computern auszubringen und ein kleines Software-Repository erstellt, das Sie zum Pushen der Aktualisierungen und zusätzlicher Software zu Ihren Client-Computern verwenden können.

Der nächste Schritt besteht darin, regelmäßige Pull- und Replizierungs-Tasks zu planen, um Ihre Quell-, Master- und verteilten Repositories zu synchronisieren, so dass all Ihre Repositories auf dem aktuellsten Stand sind. Anschließend erstellen Sie geplante Client-Aktualisierungs-Tasks, um sicherzustellen, dass Client-Software (z. B. VirusScan Enterprise) regelmäßig auf aktualisierte DAT- und Moduldateien überprüft.

Führen Sie dazu folgende Schritte aus:

1 *Planen eines Pull-Tasks, um Ihr Master-Repository täglich zu aktualisieren*.

2 *Planen eines Replikations-Tasks zum Aktualisieren Ihres verteilten Repositorys*.

3 *Planen eines Client-Aktualisierungs-Tasks, um DATs täglich zu aktualisieren*.

1 Planen eines Pull-Tasks, um Ihr Master-Repository täglich zu aktualisieren

Pull-Tasks aktualisieren Ihr Master-Software-Repository mit den aktuellsten DAT- und Moduldateien vom Quell-Repository. Standardmäßig ist Ihr Quell-Repository die McAfee-Website. Erstellen Sie einen geplanten Pull-Task, um die neuesten Aktualisierungen von der McAfee-Website einmal pro Tag abzurufen.

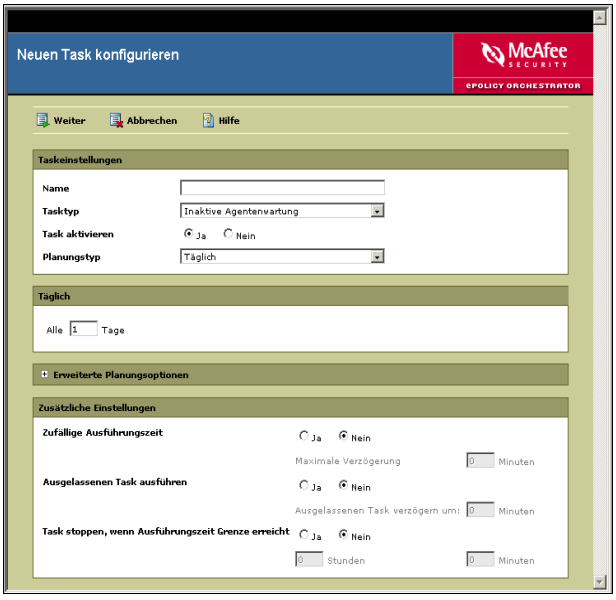
So planen Sie einen Pull-Task:

1 Wählen Sie in der Konsolenstruktur die Option **Repository** aus.

2 Klicken Sie auf der Seite **Repository** auf **Pull-Tasks planen**, um die Seite **Server-Tasks konfigurieren** zu öffnen.

3 Wählen Sie **Task erstellen** aus, um die Seite **Neuen Task konfigurieren** zu öffnen.

Abbildung 1-14 Seite "Neuen Task konfigurieren"



4 Geben Sie im Feld **Name** einen Namen ein, z. B. *Täglicher Repository-Pull-Task*.

5 Wählen Sie im Dropdownmenü **Tasktyp** die Option **Repository-Pull** aus.

6 Vergewissern Sie sich, dass **Task aktivieren** auf **Ja** gesetzt ist.

7 Wählen Sie in der Dropdown-Liste **Planungstyp** die Option **Täglich** aus.

8 Erweitern Sie **Erweiterte Planungsoptionen**, und planen Sie den Tag und Zeitpunkt für die Ausführung des Tasks.

9 Klicken Sie oben auf der Seite auf **Weiter**.

10 Wählen Sie in der Dropdown-Liste **Quell-Repository** die Option **NAIHttp** aus.

11 Belassen Sie den Zielzweig bei **Aktuell**.

12 Wenn Sie ältere Versionen von McAfee-Produkten (z. B. VirusScan 4.5.1) in Ihrem Testnetzwerk haben, wählen Sie **Unterstützung für Legacy-Produktaktualisierung** aus.

13 Klicken Sie auf **Fertig stellen**. Warten Sie, während der Task erstellt wird.

Der neue Pull-Task wird der Seite **Server-Tasks konfigurieren** hinzugefügt.

2 Planen eines Replikations-Tasks zum Aktualisieren Ihres verteilten Repositorys

Anhand Ihres neuen Pull-Tasks ist Ihr ePolicy Orchestrator-Server so konfiguriert, dass er automatisch das Master-Repository mit den neuesten Aktualisierungen vom Quell-Repository auf der McAfee-Website aktualisiert. Der Task wird einmal pro Tag ausgeführt und hält Ihr Master-Repository stets auf dem neuesten Stand.

Ein Master-Repository ist für keinen der Client-Computer auf Ihrem Netzwerk von Nutzen, die ihre Aktualisierungen von einem verteilten Repository erhalten, z. B. Computer auf dem Standort **Container1** in unserem Beispielnetzwerk. Der nächste Schritt besteht demzufolge darin sicherzustellen, dass die Aktualisierungen, die Ihrem Master-Repository hinzugefügt wurden, automatisch in Ihr verteiltes Repository repliziert werden. Hierzu erstellen Sie einen automatischen Replikations-Task, der jeden Tag eine Stunde nach dem geplanten Pull-Task ausgeführt werden soll.

So planen Sie einen automatischen Replikations-Task:

1 Wählen Sie in der Konsolenstruktur die Option **Repository** aus.

2 Klicken Sie auf der Seite **Repository** auf **Pull-Tasks planen**, um die Seite **Server-Tasks konfigurieren** zu öffnen.

3 Wählen Sie **Task erstellen** aus, um die Seite **Neuen Task konfigurieren** zu öffnen. Dies ist dieselbe Seite, die Sie für die Planung des automatischen Pull-Tasks verwendet haben.

4 Geben Sie im Feld **Name** einen Namen ein, z. B. *Täglicher Replikations-Task von verteiltem Repository*.

5 Wählen Sie in der Dropdownliste **Tasktyp** die Option **Repository-Replizierung** aus.

6 Vergewissern Sie sich, dass **Task aktivieren** auf **Ja** gesetzt ist.

7 Wählen Sie in der Dropdown-Liste **Planungstyp** die Option **Täglich** aus.

8 Erweitern Sie **Erweiterte Planungsoptionen**, und planen Sie den Tag und Zeitpunkt für die Ausführung des Tasks. Setzen Sie den Zeitpunkt auf eine Stunde nach Beginn des geplanten Pull-Tasks fest. Damit sollte dem Pull-Task genügend Zeit zur Verfügung stehen, dass er abgeschlossen werden kann. Abhängig von Ihren Netzwerk- und Internet-Verbindungen benötigt Ihr Pull-Task mehr oder weniger Zeit. Legen Sie deshalb den Beginn Ihres Replikations-Tasks entsprechend fest.

9 Klicken Sie oben auf der Seite auf **Weiter**.

10 Wählen Sie **Inkrementelle Replikation** aus, und klicken Sie auf **Fertig stellen**. Warten Sie, während der Task erstellt wird.

Der neue Replikations-Task wird in der Tabelle **Server-Tasks konfigurieren** mit Ihrem geplanten Pull-Task angezeigt.

3 Planen eines Client-Aktualisierungs-Tasks, um DATs täglich zu aktualisieren

Nachdem alle Repositories aktualisiert wurden, planen Sie einen Client-Aktualisierungs-Task, um sicherzustellen, dass VirusScan Enterprise die neuesten DAT- und Moduldateien erhält, sobald diese in Ihren Repositories sind.

Sie können den zuvor erstellten Client-Aktualisierungs-Task verwenden, nachdem Sie VirusScan Enterprise ausgebracht haben (siehe hierzu *Aktualisieren von DAT-Dateien mit einer geplanten Client-Aktualisierung* auf Seite 40). Ändern Sie einfach die Planung dieses Tasks von **Sofort ausführen** in **Täglich**, und legen Sie den Zeitpunkt auf eine Stunde nach Beginn des Replikations-Tasks fest.

SCHRITT 10

Testen von globaler Aktualisierung mit SuperAgents

Globale Aktualisierung bezeichnet eine neue Funktion in ePolicy Orchestrator 3.5, mit der Sie alle Client-Computer automatisch aktualisieren können, sobald neue Aktualisierungen im Master-Repository eingecheckt werden. Bei jeder am Master-Repository vorgenommenen Änderung repliziert ePolicy Orchestrator den Inhalt automatisch auf alle vorhandenen verteilten Repositories. Dann werden alle im Netzwerk ausgebrachten Agenten darüber benachrichtigt, dass ihre verwalteten Produkte (z. B. VirusScan Enterprise 8.0i.) sofort einen Aktualisierungs-Task durchführen müssen.

Bei einem Virenbefall kann sich die globale Aktualisierung als sehr nützlich erweisen. Angenommen, das AVERT-Team von McAfee hat als Reaktion auf einen kürzlich entdeckten Virus aktualisierte DATs veröffentlicht. Wenn Sie die globale Aktualisierung aktiviert haben, initiieren Sie einfach von der ePolicy Orchestrator-Konsole einen Pull-Task, um das Master-Software-Repository mit den neuen DAT-Dateien zu aktualisieren. Die globale Aktualisierungsfunktion von ePolicy Orchestrator erledigt den Rest – aktualisiert also innerhalb von einer Stunde die DATs aller Computer, auf denen aktive und im Netzwerk kommunizierende Agenten ausgeführt werden.

Verwenden von SuperAgents, um alle Agenten auf dem Netzwerk zu reaktivieren

ePolicy Orchestrator verwendet einen so genannten SuperAgent, um eine globale Aktualisierung zu initiieren. SuperAgents sind ePolicy Orchestrator-Agenten, die auch andere Agenten reaktivieren können, die sich im selben Netzwerksubnet befinden. Wenn in jedem Netzwerksubnet ein SuperAgent installiert ist, senden Sie eine SuperAgent-Reaktivierung an Ihre SuperAgents und anschließend an die ePolicy Orchestrator-Agenten in diesem Subnet. Die regulären Agenten können sich anschließend beim ePolicy Orchestrator-Server bezüglich Richtlinienanleitungen zurückmelden und Client-Software aktualisieren.

SuperAgents können auch als verteilte Repositories gelten. Diese SuperAgent-Repositories verwenden ein proprietäres McAfee-Replikationsprotokoll (genannt SPIPE) und können von Ihnen erstellte andere per HTTP, FTP oder UNC verteilte Repositories entweder ersetzen oder ergänzen. Dieses Handbuch enthält jedoch keine Informationen zu SuperAgent-Repositories. Informationen zu SuperAgent-Repositories finden Sie im *ePolicy Orchestrator 3.5 Produkthandbuch*.

So aktivieren Sie die globale Aktualisierung:

1 *Ausbringen eines SuperAgent auf jedes Subnet*.

2 *Aktivieren der globalen Aktualisierung auf dem ePolicy Orchestrator-Server*.

1 Ausbringen eines SuperAgent auf jedes Subnet

Sie können einen SuperAgent auf jedem Computer in Ihrem ePolicy Orchestrator-**Verzeichnis** ausbringen. Sie können auch jeden regulären ePolicy Orchestrator-Agenten in einen SuperAgent umwandeln. Verwenden Sie dazu die Richtlinienseiten des ePolicy Orchestrator-Agenten in der ePolicy Orchestrator-Konsole. Da Sie nur einen SuperAgent pro Netzwerk benötigen, stellen Sie sicher, dass Sie SuperAgents für einzelne Computer in Ihrem **Verzeichnis** und nicht für ganze Gruppen oder Standorte konfigurieren, wie sie es bei der Ausbringung regulärer Agenten oder von VirusScan Enterprise getan haben.

Im Beispielnetzwerk dieses Handbuchs würden wir einen SuperAgent auf dem Domäne1-Standort ausbringen.

Sie können einen SuperAgent auf einem Computer ausbringen, der derzeit keinen Agenten hat oder vorhandene reguläre Agenten in SuperAgents umwandeln. In unserem Beispiel ist dies durch die Richtlinienänderung für einen Agenten auf einem Computer möglich. Führen Sie dazu folgende Schritte aus:

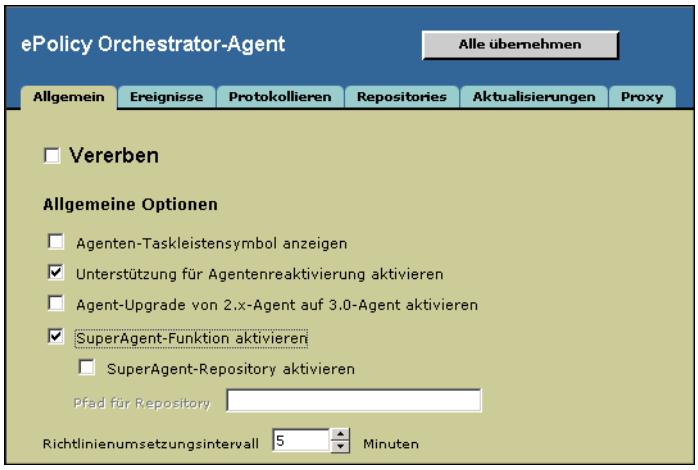
1 Wählen Sie einen bestimmten Computer im **Verzeichnis** aus.

2 Klicken Sie auf der Registerkarte **Richtlinien** auf **ePolicy Orchestrator Agent** | **Konfiguration**, um die Agenten-Richtlinienseite anzuzeigen.

3 Deaktivieren Sie auf der Registerkarte **Allgemein** die Option **Vererben**.

4 Wählen Sie **SuperAgent-Funktion aktivieren** aus.

Abbildung 1-15 Registerkarte "Allgemein"



Sie können auch ein SuperAgent-Repository auf dem Computer erstellen. Diese sind für globale Aktualisierungen jedoch nicht erforderlich und werden in diesem Handbuch nicht behandelt. Informationen zu SuperAgent-Repositories finden Sie im *ePolicy Orchestrator 3.5 Produkthandbuch*.

5 Klicken Sie auf **Alle übernehmen**, um die Richtlinienänderungen zu speichern.

6 Klicken Sie mit der rechten Maustaste auf **Verzeichnis**, und wählen Sie die Option **Agentenreaktivierung** aus.

7 Stellen Sie den Wert für **Intervall für Agenten-Zufallsgenerator** auf **0** Minute ein, und klicken Sie auf **OK**.

8 Wiederholen Sie diese Schritte, wenn Sie über Computer in anderen Netzwerksubnets verfügen.

Warten Sie, während der SuperAgent erstellt wird. Sobald er aktiviert ist, sieht das Taskleistensymbol auf dem Host-Computer des SuperAgent etwas anders aus.

Sie können diese SuperAgents verwenden, um andere Agenten im lokalen Subnet zu reaktivieren. Dadurch sparen Sie Bandbreite, besonders in einem großen Netzwerk mit vielen remoten, über WAN verbundenen, Standorten. Senden Sie Reaktivierungen an einige SuperAgents, und lassen Sie diese die anderen Agenten im lokalen LAN reaktivieren. SuperAgents spielen eine wichtige Rolle bei der neuen globalen Aktualisierungsfunktion.

2 Aktivieren der globalen Aktualisierung auf dem ePolicy Orchestrator-Server

Diese Funktion kann über die ePolicy Orchestrator-Konsole ein- oder ausgeschaltet werden. Ist sie aktiv, wird durch Änderungen am Master-Repository die automatische Replizierung auf verteilten Repositories, falls vorhanden, ausgelöst. Danach folgt eine SuperAgent-Reaktivierung für das gesamte **Verzeichnis**. Die SuperAgents wiederum aktivieren Agenten in ihren lokalen Subnets.

So schalten Sie die globale Aktualisierung ein:

1. Wählen Sie in der Konsolenstruktur Ihren ePolicy Orchestrator-Server aus.
2. Klicken Sie im Detailbereich auf die Registerkarte **Einstellungen**.
3. Setzen Sie unten auf der Seite **Servereinstellungen** den Wert für **Globale Aktualisierung aktivieren** auf **Ja**.
4. Ändern Sie die Option **Zufälliges Intervall für globale Aktualisierung** für diese Überprüfung auf **1** Minute.
5. Belassen Sie die Standardeinstellungen unter **Signaturen und Module**.
6. Wählen Sie unter **Patches und Service Packs** die Option **VirusScan Enterprise 8.0** aus.
7. Klicken Sie auf **Einstellungen übernehmen**, um die Änderung zu speichern.

Nachdem die SuperAgents auf Subnets Ihres Netzwerkes ausgebracht wurden und die globale Aktualisierung aktiviert wurde, werden die Änderungen automatisch in Ihre Repositories repliziert, wenn Sie Ihr Master-Repository ändern. Wenn die Replikation abgeschlossen ist, sendet der ePolicy Orchestrator-Server eine SuperAgent-Reaktivierung an die SuperAgents. Der SuperAgent sendet wiederum eine Reaktivierung an alle Agenten im lokalen Subnet. Diese Agenten checken mit dem Server ein und laden Richtlinienänderungen herunter. Zwischen dem Einchecken der Änderungen in das Master-Repository und dem Empfangen der Aktualisierung auf dem letzten Client-Computer sollte nicht mehr als eine Stunde liegen.

SCHRITT 11

Wie geht es jetzt weiter?

Sie haben nun die meisten zentralen Funktionen des ePolicy Orchestrator 3.5.0. kennen gelernt. Selbstverständlich können Sie darüber hinaus noch zahlreiche weitere Funktionen von ePolicy Orchestrator und VirusScan Enterprise nutzen. Zusätzliche Informationen zu erweiterten Funktionen finden Sie im *ePolicy Orchestrator 3.5 Produkthandbuch*, dem *VirusScan Enterprise 8.0i Produkthandbuch*, und dem *VirusScan Enterprise 8.0i Konfigurationshandbuch für ePolicy Orchestrator 3.5.* Diese und andere hilfreiche Ressourcen stehen auf der McAfee-Website zum Download bereit.

Testen der Funktionen

In diesem Abschnitt des *Handbuchs zur Testversion* wird dargestellt, wie Sie zwei der im vorherigen Abschnitt nicht behandelten neuen Funktionen einrichten und verwenden können:

- *ePolicy Orchestrator-Benachrichtigung*.
- *Entdeckung nicht autorisierter Systeme* auf Seite 55.

ePolicy Orchestrator-Benachrichtigung

Echtzeit-Informationen über Bedrohungen und Konformitäten in Ihrem Netzwerk sind ausschlaggebend für Ihren Erfolg.

Sie können in ePolicy Orchestrator Regeln konfigurieren, um benachrichtigt zu werden, wenn benutzerdefinierte Ereignisse in Bezug auf Bedrohungen oder Konformität vom ePolicy Orchestrator-Server empfangen und verarbeitet werden. Mithilfe einer regelbasierten Steuerung von Aggregation und Beschränkung können Sie festlegen, wann Benachrichtigungen gesendet werden und wann nicht.

Sie können eine beliebige Anzahl von Regeln erstellen, die Sie bei beinahe jedem von ihren Sicherheitsprogrammen gesendeten Ereignis in Bezug auf Bedrohungen oder Konformität benachrichtigt. In diesem Handbuch konzentrieren wir uns jedoch darauf, diese Funktion in Hinblick auf E-Mail-Benachrichtigungen bei Virus-entdeckt-Ereignissen zu erläutern.

In diesem Abschnitt des Handbuchs wenden Sie folgende Methoden an:

1. *Konfigurieren von Agentenrichtlinien, um Ereignisse sofort hochzuladen*.
2. *Konfigurieren von Benachrichtigungen*.
3. *Erstellen einer Regel für ein beliebiges VirusScan Enterprise-Ereignis*.
4. *Ermöglichen einer beispielhaften Virusentdeckung*.

SCHRITT 1

Konfigurieren von Agentenrichtlinien, um Ereignisse sofort hochzuladen

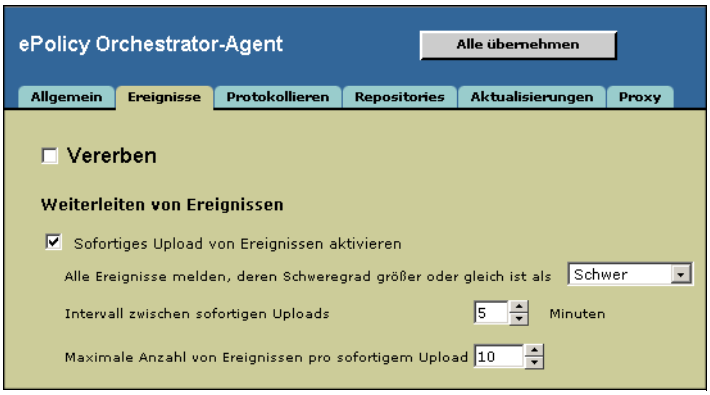
Da der Agent Ereignisse von den verwalteten Systemen aus an den ePolicy Orchestrator-Server sendet, müssen Sie die Agentenrichtlinie so konfigurieren, dass Ereignisse sofort gesendet werden. Anderenfalls erhält der ePolicy Orchestrator-Server Ereignisse erst zum nächsten Agent-zu-Server-Kommunikationsintervall (ASKI).

1 Klicken Sie in der Konsolenstruktur auf **Verzeichnis** und anschließend im oberen Detailbereich auf die Registerkarte **Richtlinien**.

2 Wählen Sie im oberen Abschnitt des Detailbereichs die Option **ePolicy Orchestrator Agent** | **Konfiguration** aus.

3 Deaktivieren Sie auf der Registerkarte **Ereignisse** im unteren Detailbereich die Option **Vererben**.

Abbildung 2-1 Registerkarte "Ereignisse"



4 Wählen Sie **Sofortiges Upload von Ereignissen aktivieren** aus, und klicken Sie anschließend auf **Alle übernehmen**.

Damit haben Sie die Agenten so konfiguriert, dass Ereignisse sofort zum ePolicy Orchestrator-Server gesendet werden, und können nun die ePolicy Orchestrator-Benachrichtigungen konfigurieren.

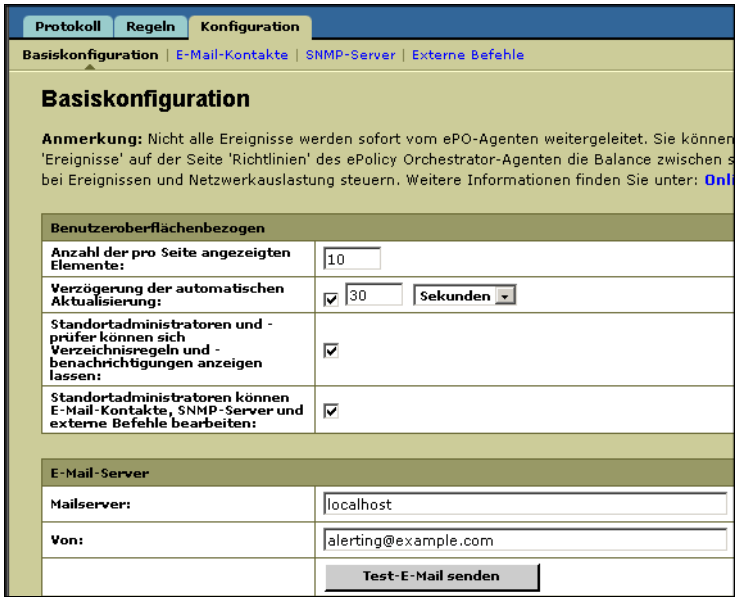
SCHRITT 2

Konfigurieren von Benachrichtigungen

Vor dem Festlegen von Regeln müssen Sie zunächst bestimmen, welche Personen die Benachrichtigungen erhalten sollen, in welchem Format diese sein sollen und was kommuniziert werden soll:

1 Klicken Sie in der Konsolenstruktur auf **Benachrichtigungen**, und wählen Sie anschließend im Detailbereich die Registerkarte **Konfiguration** | **Basiskonfiguration** aus.

Abbildung 2-2 Basiskonfiguration



2 Geben Sie unter **E-Mail-Server** den Namen eines Mailservers an, an den der ePolicy Orchestrator-Server Nachrichten leiten kann, sowie die E-Mail-Adresse, die in der **Von**-Zeile der Nachricht angezeigt werden soll.

Wenn Sie entscheiden, welche E-Mail-Adresse in dieses Feld eingetragen werden soll, überlegen Sie auch, wie viele Administratoren Nachrichten erhalten sollen und ob Sie ihnen das Senden von Antworten ermöglichen möchten.

3 Klicken Sie auf **Anwenden** und anschließend im oberen Bereich der Registerkarte auf **E-Mail-Kontakte**. Auf dieser Seite können Sie alle Adressen angeben, die in das Adressbuch, aus dem Sie bei der Regelerstellung Empfänger auswählen, eingefügt werden sollen.

Ein Kontakt sollte in der Liste bereits vorhanden sein: **Administrator**. Die für **Administrator** hinterlegte E-Mail-Adresse ist diejenige, die Sie im Installationsassistenten im Feld **E-Mail-Adresse einstellen** angegeben haben. Wenn Sie den im Assistenten vorgegebenen Standardwert nicht geändert haben, lautet die Adresse **Administrator@beispiel.com**. Wenn es sich bei der Adresse für **Administrator** um eine für den Empfang und den Versand von E-Mails nicht funktionierende Adresse handelt, klicken Sie darauf, und geben Sie eine Adresse an, unter der Sie E-Mails empfangen und versenden können.

Sie können auf der Registerkarte **Konfiguration** auch SNMP-Server konfigurieren, über die Sie SNMP-Traps empfangen möchten, sowie externe Befehle, die ausgeführt werden sollen, wenn bestimmte Ereignisse empfangen werden. Diese Themen sind außerhalb der Zielsetzung dieses Handbuchs. Weitere Informationen hierzu erhalten Sie im *ePolicy Orchestrator 3.5 Produkthandbuch*.

Nachdem Sie einen E-Mail-Server und eine E-Mail-Adresse für den Nachrichtenversand angegeben haben, können Sie nun eine Regel erstellen, die bei einem VirusScan Enterprise-Ereignis ausgeführt wird.

SCHRITT 3

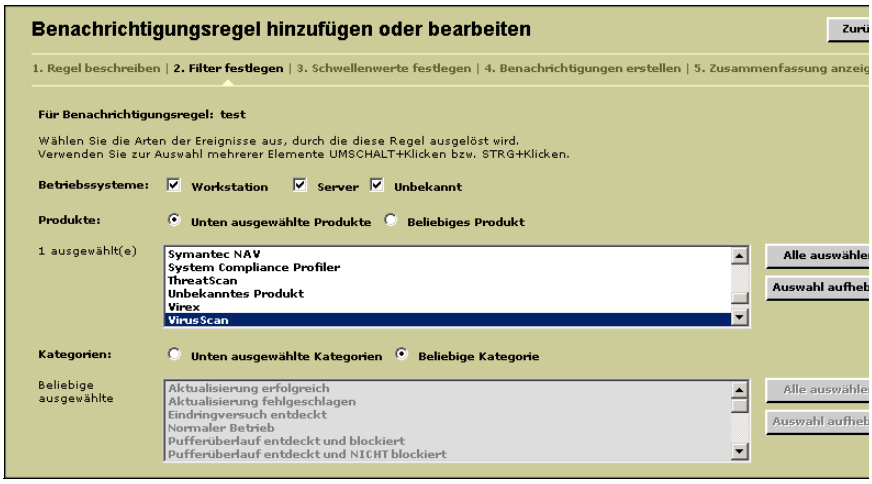
Erstellen einer Regel für ein beliebiges VirusScan Enterprise-Ereignis

Sie können eine Vielzahl von Regeln erstellen, die auf beinahe jede von Ihren verwalteten Sicherheitsprogrammen erhaltene Ereigniskategorie reagieren. Weitere Informationen finden Sie im von *ePolicy Orchestrator 3.5 Produkthandbuch* in *Kapitel 12: ePolicy Orchestrator-Benachrichtigung*.

1. Wählen Sie die Registerkarte **Regeln** aus, und klicken Sie auf **Regel hinzufügen**, um den Assistenten **Benachrichtigungsregel hinzufügen oder bearbeiten** zu starten.
2. Behalten Sie auf der Seite **Regel beschreiben** im Textfeld **Definiert** den Standardwert (**Verzeichnis**) bei. Sie können Regeln für das **Verzeichnis** oder jeden Standort innerhalb des **Verzeichnisses** erstellen.
3. Geben Sie in das Textfeld **Regelname** einen Namen für die Regel ein, z. B. **Virus gefunden**.
4. Geben Sie in das Textfeld **Beschreibung** eine Beschreibung für die Regel ein, z. B. **Viren von VirusScan Enterprise entdeckt**. Klicken Sie anschließend auf **Weiter**.
5. Gehen Sie auf der Seite **Filter festlegen** folgendermaßen vor:
   a. Lassen Sie alle Kontrollkästchen **Betriebssysteme** markiert.
   b. Wählen Sie unter **Produkte** die Option **VirusScan** aus.
   c. Wählen Sie unter **Kategorien** oberhalb der Liste die Option **Beliebige Kategorie** aus, und klicken Sie auf **Weiter**.

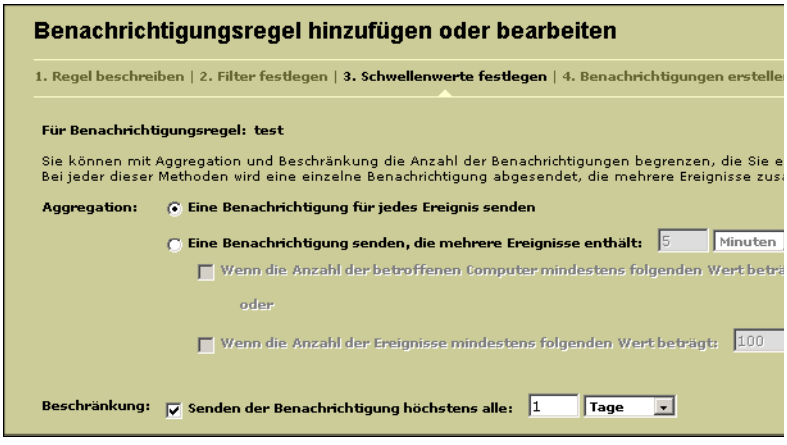
In der bislang vorgenommenen Konfiguration wird die Regel auf jedes VirusScan-Ereignis angewendet, das auf jedem verwalteten System innerhalb des **Verzeichnisses** auftritt.

Abbildung 2-3 Seite "Filter festlegen"


Benachrichtigungsregel hinzufügen oder bearbeiten
1. Regel beschreiben | 2. Filter festlegen | 3. Schwellenwerte festlegen | 4. Benachrichtigungen erstellen | 5. Zusammenfassung anzeig
Für Benachrichtigungsregel: test
Wählen Sie die Arten der Ereignisse aus, durch die diese Regel ausgelöst wird.
Verwenden Sie zur Auswahl mehrerer Elemente UMSCHALT+Klicken bzw. STRG+Klicken.
Betriebssysteme: Workstation Server Unbekannt
Produkte: Unten ausgewählte Produkte Beliebiges Produkt
1 ausgewählt(e)
Symantec NAV
System Compliance Profiler
ThreatScan
Unbekanntes Produkt
Virex
VirusScan
Kategorien: Unten ausgewählte Kategorien Beliebige Kategorie
Beliebige ausgewählte
Aktualisierung erfolgreich
Aktualisierung fehlgeschlagen
Eindringversuch entdeckt
Normaler Betrieb
Pufferüberlauf entdeckt und blockiert
Pufferüberlauf entdeckt und NICHT blockiert

6 Für diesen Task verwenden Sie die auf dieser Seite ausgewählten Standardwerte. Sie können jedoch auf der Seite **Schwellenwerte festlegen** die Anzahl der Benachrichtigungen begrenzen, die Sie aufgrund der Regel empfangen. Sie können beispielsweise eine beliebige Regel so festlegen, dass Ihnen nur dann eine Benachrichtigung gesendet werden soll, wenn die Anzahl der betroffenen Computer einen bestimmten Wert innerhalb eines bestimmten Zeitraums erreicht (**Aggregation**). Weiterhin können Sie die Anzahl an gesendeten Benachrichtigungen begrenzen, indem Sie angeben, dass weitere Nachrichten erst nach einer bestimmten Zeitspanne empfangen werden sollen (**Beschränkung**). McAfee empfiehlt in den allermeisten Fällen die Beschränkungsfunktion, um bei einem Virenausbruch eine Benachrichtigungsflut zu vermeiden.

Abbildung 2-4 Seite "Schwellenwerte festlegen"


Benachrichtigungsregel hinzufügen oder bearbeiten
1. Regel beschreiben | 2. Filter festlegen | 3. Schwellenwerte festlegen | 4. Benachrichtigungen erstelle
Für Benachrichtigungsregel: test
Sie können mit Aggregation und Beschränkung die Anzahl der Benachrichtigungen begrenzen, die Sie e
Bei jeder dieser Methoden wird eine einzelne Benachrichtigung abgesendet, die mehrere Ereignisse zus
Aggregation: Eine Benachrichtigung für jedes Ereignis senden
Eine Benachrichtigung senden, die mehrere Ereignisse enthält: 5 Minuten
Wenn die Anzahl der betroffenen Computer mindestens folgenden Wert beträ
oder
Wenn die Anzahl der Ereignisse mindestens folgenden Wert beträgt: 100
Beschränkung: Senden der Benachrichtigung höchstens alle: 1 Tage

Lassen Sie die Option **Eine Benachrichtigung für jedes Ereignis senden** ausgewählt, und klicken Sie auf **Weiter**.

7 Klicken Sie auf der Seite **Benachrichtigungen erstellen** auf **E-Mail-Nachricht hinzufügen**.

8 Klicken Sie im Feld links auf der Seite auf **Administrator** und anschließend auf **An**. **Administrator** wird in das Feld **Benachrichtigungsempfänger** verschoben.

Damit legen Sie fest, dass die Benachrichtigung, die Sie gerade konfigurieren, an die in Schritt 2: *Konfigurieren von Benachrichtigungen* auf Seite 51 (für den Kontakt **Administrator**) eingegebene Adresse gesendet wird.

9 Geben Sie einen **Betreff** für die E-Mail ein, die bei der Auslösung dieser Regel an **Administrator** gesendet wird, z. B. **Bedrohung von VirusScan entdeckt**.

10 Geben Sie einen **Nachrichtentext** für die E-Mail ein, die bei der Auslösung dieser Regel gesendet wird, z. B. **VirusScan hat eine Bedrohung entdeckt**.

11 Sie können in den Nachrichtentext unterschiedliche Variablen einfügen, so dass in der Benachrichtigung wichtige Informationen aus den Ereignisdateien enthalten sind.

Wählen Sie für den in diesem Handbuch beschriebenen Zweck **Betroffene Computernamen** aus, und klicken Sie auf **Nachrichtentext**. Dadurch wird der Name des betroffenen Computers, sofern er in der Ereignisdatei aufgeführt ist, in den Text der E-Mail-Nachricht eingefügt. Klicken Sie auf **Speichern**.

Auf der Seite **Benachrichtigungen erstellen** können Sie eine Vielzahl an Nachrichten in unterschiedlichen Formaten für mehrere Empfänger erstellen sowie externe Befehle auswählen, die ausgeführt werden sollen. Dies geht über die Zielsetzung dieses Dokuments hinaus. Weitere Informationen hierzu finden Sie im *ePolicy Orchestrator 3.5 Produkthandbuch*.

12 Klicken Sie auf **Weiter**, überprüfen Sie auf der Seite **Zusammenfassung anzeigen** die Konfiguration der von Ihnen erstellten Regel, und klicken Sie anschließen auf **Fertig stellen**.

SCHRITT 4

Ermöglichen einer beispielhaften Virusentdeckung

Sie haben nun die Konfiguration der Funktion abgeschlossen und eine Regel erstellt, die bei Ereignisdateien von VirusScan Enterprise ausgelöst wird. Jetzt benötigen Sie noch eine Ereignisdatei, die die Regel auslöst.

1 Laden Sie die Datei EICAR.COM auf einen der Workstation-Testcomputer herunter. Jedes Mal, wenn Sie diese Datei herunterladen, wird eine Test-Virusentdeckung erstellt. Zum Zeitpunkt der Veröffentlichung war diese Datei auf der Website von EICAR.ORG erhältlich:

http://www.eicar.org/anti_virus_test_file.htm

Diese Datei ist *kein* Virus.

2 Wenn EICAR.COM heruntergeladen wird, entdeckt der Zugriffs-Scanner den EICAR-Testvirus und versetzt ihn in Quarantäne. Außerdem wird eine Ereignisdatei mit dieser Information an den ePolicy Orchestrator-Server gesendet.

3 Innerhalb weniger Minuten wird eine Benachrichtigung erstellt und an den Posteingang des E-Mail-Benachrichtigungsempfängers gesendet, den Sie zuvor angegeben haben.

Sie haben das Produkt erfolgreich zum Versenden von Nachrichten an eine bestimmte Person eingerichtet. Sie haben eine Regel erstellt, um Benachrichtigungen auf der Grundlage von Ereignissen von VirusScan Enterprise zu versenden, und Sie haben die Regel auf korrekte Funktion hin überprüft. Herzlichen Glückwunsch!

Entdeckung nicht autorisierter Systeme

In jedem verwalteten Netzwerk gibt es jederzeit zwangsläufig eine kleine Anzahl Systeme, die nicht über einen ePolicy Orchestrator-Agenten verfügen. Das können Computer sein, die sich häufig am Netzwerk an- oder abmelden, z. B. Testserver, Laptop-Computer oder drahtlose Geräte. Außerdem gibt es Endbenutzer, die Agenten auf ihren Computern deinstallieren oder deaktivieren. Diese ungeschützten Systeme sind die Achillesferse jeder Antivirus- und Sicherheitsstrategie und die Eintrittspunkte, über die Viren und andere potenziell schädliche Programme auf das Netzwerk zugreifen können.

Das System zur Entdeckung nicht autorisierter Systeme hilft bei der Überwachung *aller* Systeme des Netzwerks, d. h. nicht nur der Systeme, die bereits von ePolicy Orchestrator verwaltet werden, sondern auch der nicht autorisierten Systeme. Unter einem *nicht autorisierten System* ist jeder Computer zu verstehen, der derzeit nicht von einem ePolicy Orchestrator-Agenten verwaltet wird, aber verwaltet werden sollte. Der ePolicy Orchestrator-Server bietet eine Entdeckung nicht autorisierter Systeme, um eine Entdeckung von nicht autorisierten Systemen in Echtzeit über einen Sensor zu gewährleisten, der auf jedem Netzwerkübertragungssegment platziert ist. Der Sensor empfängt Netzwerkübertragungsmeldungen und erkennt, wenn sich ein neuer Computer mit dem Netzwerk verbunden hat.

Sobald der Sensor ein neues System im Netzwerk entdeckt, sendet er eine Meldung an den Server für die Entdeckung nicht autorisierter Systeme. Der Server für die Entdeckung nicht autorisierter Systeme überprüft dann beim ePolicy Orchestrator-Server, ob auf dem neu entdeckten Computer ein aktiver Agent installiert ist und ob der Computer von ePolicy Orchestrator verwaltet wird. Kennt ePolicy Orchestrator den neuen Computer noch nicht, ermöglicht die Entdeckung nicht autorisierter Systeme eine Reihe von Schritten zur erneuten Vermittlung, einschließlich der Warnung von Netzwerk- und Antivirus-Administratoren oder der automatischen Übertragung eines ePolicy Orchestrator-Agenten auf den Computer per Push-Verfahren.

In diesem Abschnitt des *Handbuchs zur Testversion* wenden Sie folgende Methoden an:

1 *Konfigurieren von Richtlinien zu Sensoren für die Entdeckung nicht autorisierter Systeme*.

2 *Ausbringen des Sensors für die Entdeckung nicht autorisierter Systeme*.

3 *Konfigurieren einer automatischen Antwort*.

4 *Entdecken und Behandeln nicht autorisierter Rechner*.

SCHRITT 1

Konfigurieren von Richtlinien zu Sensoren für die Entdeckung nicht autorisierter Systeme

Wenn Sie Sensoren der Entdeckung nicht autorisierter Systeme ausbringen, sollten Sie zunächst die Richtlinie des Sensors konfigurieren.

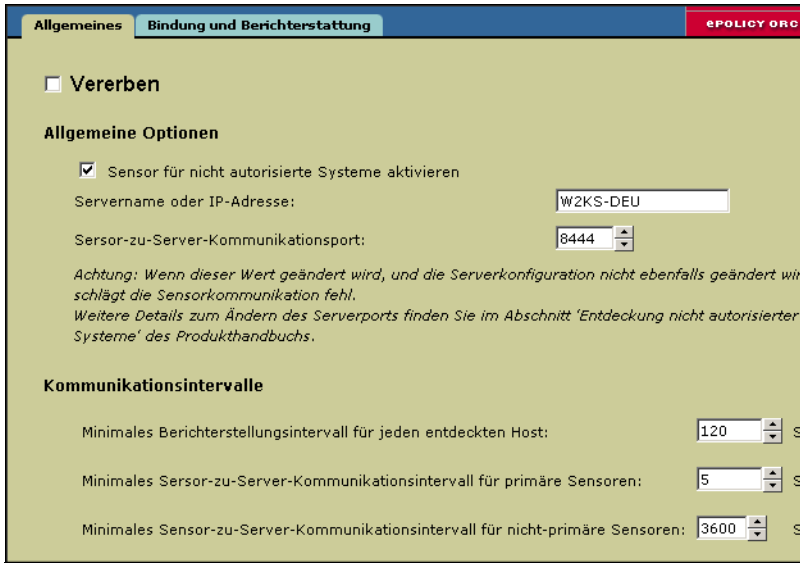
Die hier dargestellten Konfigurationen der Richtlinien für Sensoren dienen allein Testzwecken. Es handelt sich nicht um empfohlene Konfigurationen für ein Ausbringen des Sensors innerhalb einer Produktionsumgebung.

Wenn der Sensor auf ein System in Ihrer Umgebung ausgebracht wird, benötigt er jeweils ein Intervall für die Agent-zu-Server-Kommunikation und für die Richtliniendurchsetzung, um richtig zu funktionieren. Bei der Agent-zu-Server-Kommunikation wird der Sensor in deaktiviertem Zustand im System installiert. Anschließend ruft die Richtliniendurchsetzung die Richtlinie einschließlich Sicherheitszertifikaten ab. Diese Zertifikate werden benötigt, damit Sensor und Server direkt kommunizieren können.

Die im Folgenden dargestellten Konfigurationsänderungen an der Richtlinie für Sensoren beschleunigen diesen Prozess, um den Zwecken dieses Handbuchs zu genügen.

1 Klicken Sie in der Konsolenstruktur auf **Verzeichnis**, und wählen Sie anschließend im Detailbereich auf der Registerkarte **Richtlinie** die Option **Sensor für nicht autorisierte Systeme | Konfiguration** aus.

Abbildung 2-5 Sensor für nicht autorisierte Systeme | Konfiguration



2 Deaktivieren Sie **Vererben**, und nehmen Sie anschließend unter **Kommunikationsintervalle** die folgenden Änderungen vor:

   a Stellen Sie den Wert für **Minimales Berichterstellungsintervall für jeden entdeckten Host** auf **120** Sekunden ein.

   b Stellen Sie den Wert für **Minimales Sensor-zu-Server-Kommunikationsintervall für primäre Sensoren** auf **5** Sekunden ein.

3 Klicken Sie auf **Alle übernehmen**.

SCHRITT 2

Ausbringen des Sensors für die Entdeckung nicht autorisierter Systeme

Der Sensor stellt den verteilten Bereich der Architektur für die Entdeckung nicht autorisierter Systeme dar. Sensoren entdecken die Computer, Router, Drucker und anderen Netzwerkgeräte, die mit dem Netzwerk verbunden sind. Sie sammeln Informationen über die entdeckten Geräte und leiten diese an den Server für die Entdeckung nicht autorisierter Systeme weiter.

Der Sensor ist eine kleine Win32-eigene ausführbare Anwendung. Ähnlich wie ein ePolicy Orchestrator-SuperAgent muss mindestens ein Sensor in jedem Übertragungssegment ausgebracht werden. Meist handelt es sich dabei um dasselbe wie bei einem Netzwerksubnet im Netzwerk. Der Sensor kann auf jedem NT-basierten Windows-Betriebssystem ausgeführt werden, z. B. Windows 2000, Windows XP oder Windows 2003.

Weitere Informationen zum Sensor und dessen Funktionsweise finden Sie im *ePolicy Orchestrator 3.5 Produkthandbuch* in *Kapitel 11: Entdeckung nicht autorisierter Systeme*.

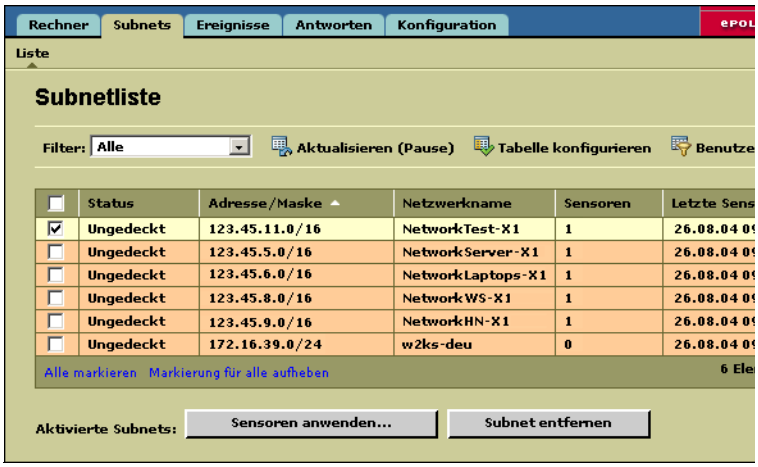
Je nach Einrichtung Ihrer Testumgebung verfügen Sie darin über mindestens ein Subnet.

So bringen Sie den Sensor aus:

1 Klicken Sie in der Konsolenstruktur auf **Entdeckung nicht autorisierter Systeme**, und wählen Sie anschließend im Detailbereich die Registerkarte **Subnets** aus, um die **Subnetliste** anzuzeigen.

2 Wählen Sie die Subnets aus, in die Sie Sensoren ausbringen möchten. Klicken Sie dazu einmal auf das Kontrollkästchen für das entsprechende Subnet und abschließend auf **Sensoren anwenden**.

Abbildung 2-6 Seite "Subnetliste"



3 Wenn die Seite **Sensoranwendung: Voreinstellungen festlegen** angezeigt wird, vergewissern Sie sich, dass die Option **Manuelle Rechnerauswahl zulassen** aktiviert ist.

4 Hier werden keine Kriterien festgelegt, mit denen ePolicy Orchestrator Sensoren automatisch ausbringen kann, Sie können jedoch mithilfe solcher Kriterien schneller entscheiden, auf welchen Systemen die Sensoren installiert werden sollen. Auf diese Weise kann ePolicy Orchestrator die für die Installation der Sensoren am besten geeigneten Systeme in jedem Subnet ermitteln.

5 Klicken Sie auf **Weiter**, und aktivieren Sie das Kontrollkästchen, das neben dem System angezeigt wird, auf dem Sie einen Sensor ausbringen möchten. Klicken Sie auf **Für die Anwendung markieren** und anschließend auf **Schließen**.

6 Klicken Sie auf der Seite **Sensoranwendung: Prüfen und genehmigen** auf **Jetzt anwenden**.

Die Seite **Aktionsfortschritt** der Registerkarte **Ereignisse** zeigt den Fortschritt jeder einzelnen Sensorausbringung an.

7 Beachten Sie, dass Sie jeweils ein Intervall für die Agent-zu-Server-Kommunikation und für die Richtliniendurchsetzung abwarten müssen, bevor der Sensor sich beim Server melden kann und richtig funktioniert. Dies kann durch das Senden von Agentenreaktivierungen beschleunigt werden.

a Klicken Sie dazu mit der rechten Maustaste in der Konsolenstruktur im **Verzeichnis** auf den Computer, auf dem Sie den Sensor installiert haben, und wählen Sie **Agentenreaktivierung** aus.

b Stellen Sie den Wert für **Intervall für Agenten-Zufallsgenerator** auf **0** Minute ein, und klicken Sie auf **OK**.

c Warten Sie 2 Minuten, und wiederholen Sie den Vorgang.

8 Wenn sich der **Aktionsstatus** in **Erfolgreich abgeschlossen** geändert hat, hat sich der Sensor beim Server gemeldet und funktioniert.

9 Wählen Sie die Registerkarte **Rechner** und anschließend **Zusammenfassung** aus, um eine Zusammenfassung der entdeckten Systeme anzuzeigen.

Sie haben nun den Sensor ausgebracht und installiert und können für die Funktion eine Reaktion auf entdeckte nicht autorisierte Systeme konfigurieren.

SCHRITT 3

Konfigurieren einer automatischen Antwort

Sie können automatische Antworten und Reaktionen konfigurieren, die ePolicy Orchestrator bei der Entdeckung nicht autorisierter Systeme ausführen soll. Diese Funktion bietet eine beträchtliche Flexibilität beim Definieren von auszuführenden Aktionen und Zuweisen von Bedingungen. Vollständige Informationen hierzu finden Sie im *ePolicy Orchestrator 3.5 Produkthandbuch* in *Kapitel 11: Entdeckung nicht autorisierter Systeme*.

In vielen Situationen möchten Sie eventuell das Ausführen automatischer Antworten unterbinden. Dazu können Sie Bedingungen für unterschiedliche Arten von nicht autorisierten Systemen erstellen, bei denen keine Aktion ausgeführt wird oder bei denen entdeckte Systeme lediglich als aktionsbedürftig markiert werden.

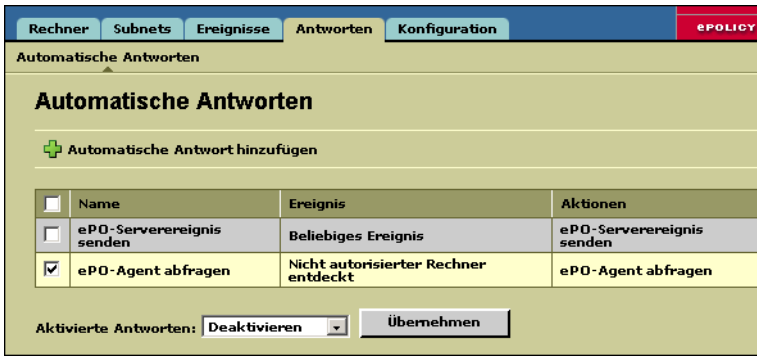
Für die in diesem Handbuch beschriebenen Zwecke erstellen Sie eine Antwort, die bei Entdeckung eines nicht autorisierten Systems eine Push-Installation des Agenten auf diesem System ausführt.

1 Klicken Sie in der Konsolenstruktur auf **Entdeckung nicht autorisierter Systeme**, und wählen Sie anschließend im Detailbereich die Registerkarte **Antworten** aus.

2 Aktivieren Sie das Kontrollkästchen neben der standardmäßigen Antwort **ePO-Agent abfragen**, wählen Sie in der Dropdown-Liste **Aktivierte Antworten** die Option **Deaktivieren** aus, und klicken Sie anschließend auf **Übernehmen**.

   Mit dieser Antwort wird das entdeckte System auf Agenten eines anderen ePolicy Orchestrator-Servers überprüft.

Abbildung 2-7 Seite "Automatische Antworten"



3 Klicken Sie auf **Automatische Antwort hinzufügen**, um die Seite **Automatische Antwort hinzufügen oder bearbeiten** anzuzeigen.

4 Geben Sie einen Namen für die Antwort ein, z. B. **Agenten-Push**.

5 Klicken Sie unter **Bedingungen** auf **Bedingung hinzufügen**, und wählen Sie in der Liste **Eigenschaft** die Option **Nicht autorisierter Typ** aus.

Abbildung 2-8 Seite "Automatische Antwort hinzufügen oder bearbeiten"

6 Wählen Sie für **Vergleich** die Option **ist** und für **Wert** die Option **Kein Agent** aus.

7 Ändern Sie unter **Aktionen** die **Methode** von der standardmäßigen Antwort **E-Mail senden** in **ePO Agent-Push**, und akzeptieren Sie die standardmäßigen **Parameter**.

8 Klicken Sie auf **OK**.

9 Die Seite **Automatische Antworten** wird wieder angezeigt. Aktivieren Sie das Kontrollkästchen neben der automatischen Antwort **Agenten-Push**. Wählen Sie in der Dropdownliste **Aktivierte Antworten** die Option **Aktivieren** aus, und klicken Sie anschließend auf **Übernehmen**.

Sie haben nun den Sensor ausgebracht und eine Reaktion auf entdeckte nicht autorisierte Systeme erstellt und aktiviert. Jetzt können jetzt ein solches nicht autorisiertes System erstellen.

SCHRITT 4

Entdecken und Behandeln nicht autorisierter Rechner

Sie müssen nun ein System ohne Agenten in die Testumgebung einführen. Dies kann unterschiedlich durchgeführt werden, z. B. durch das Beitreten eines Laptops in das Testnetzwerk oder durch das Verschieben eines Computers aus einer externen Domäne in die zuvor erstellte Testdomäne.

1. Fügen Sie einen Computer ohne ePolicy Orchestrator-Agent zum Testnetzwerk hinzu.
2. Klicken Sie auf der Registerkarte **Rechner** auf **Liste**. Sobald der Sensor ein nicht autorisiertes System entdeckt, sendet er eine Meldung an den Server und trägt das System in die **Rechnerliste** ein.
3. Sobald es in der Liste angezeigt wird, können Sie eine 5-minütige Pause einlegen und die Agenten-Installation abwarten.
4. Sobald die Agenteninstallation abgeschlossen ist, ist der Wert für **Nicht autorisierter Typ** des Systems **Verwaltet**.

   Damit ist dieser Vorgang noch nicht abgeschlossen. Sie müssen das nun verwaltete System an seinem entsprechenden Speicherort im **Verzeichnis** ablegen.
5. Wenn sich der Wert für **Nicht autorisierter Typ** des Systems in **Verwaltet** geändert hat, wird es in der Konsolenstruktur unter **Verzeichnis** | **Lost&Found** | **Nicht autorisierte Systeme** abgelegt.

   Das Verzeichnis **Lost&Found** ist ein Aufbewahrungsort für Systeme, die von ePolicy Orchestrator erkannt, aber nicht an eine bestimmte Stelle innerhalb des **Verzeichnisses** abgelegt werden konnten.
6. Klicken Sie auf das System, und ziehen Sie es bei gedrückter Maustaste an den gewünschten Standort oder die gewünschte Gruppe in Ihrem ePolicy Orchestrator-**Verzeichnis**.

Sie haben den Sensor erfolgreich konfiguriert und ausgebracht, eine automatische Antwort erstellt, die für das von Ihnen eingeführte nicht autorisierte System durchgeführt wurde, und ein neues verwaltetes System an der richtigen Stelle im **Verzeichnis** abgelegt. Herzlichen Glückwunsch!